BINGHAM MCCUTCHEN LLP
Jonathan Loeb (#162758) jonathan.loeb@bingham.com
Jeffrey Rosenfeld (#221625) jeffreyrosenfeld@bingham.com
Edward Andrews (#268479) edward.andrews@bingham.com
The Water Garden, Suite 2050 North
1601 Cloverfield Boulevard
Santa Monica, CA 90404-4082
Telephone: 310-907-1000
Facsimile: 310-907-2000

AMERICAN CIVIL LIBERTIES UNION FOUNDATION
OF NORTHERN CALIFORNIA
Linda Lye (#215584) llye@aclunc.org
Julia Harumi Mass (#189649) jmass@aclunc.org
39 Drumm Street
San Francisco, CA 94111
Telephone: 415-621-2493
Facsimile: 415-255-8437

ASIAN AMERICANS ADVANCING
JUSTICE - ASIAN LAW CAUCUS
Nasrina Bargzie (#238917) nasrinab@advancingjustice-alc.org
Yaman Salahi (#288752) yamans@advancingjustice-alc.org
55 Columbus Avenue
San Francisco, CA 94111
Telephone: 415-848-7711
Facsimile: 415-896-1702

Attorneys for PlaintiffsWiley Gill, James Prigoff, Tariq Razak, Khaled Ibrahim, and Aaron Conklin

Additional counsel listed on signature page

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
SAN FRANCISCO-OAKLAND DIVISION

WILEY GILL; JAMES PRIGOFF; TARIQ RAZAK; KHALED IBRAHIM; and AARON CONKLIN,

Plaintiffs,

v.

DEPARTMENT OF JUSTICE; ERIC H. HOLDER, Jr., in his official capacity as the Attorney General of the United States; PROGRAM MANAGER - INFORMATION SHARING ENVIRONMENT; KSHEMENDRA PAUL, in his official capacity as the Program Manager of the Information Sharing Environment,

Defendants.

No. ___________________

COMPLAINT FOR DECLARATORY AND INJUNCTIVE RELIEF

Administrative Procedure Act Case

INTRODUCTION

1. This complaint challenges a widespread domestic surveillance program that targets constitutionally protected conduct and encourages racial and religious profiling. Plaintiffs are five United States citizens – two photographers, one white man who is a devout Muslim, and two men of Middle Eastern and South Asian descent. They engaged in innocuous, lawful, and in some cases First Amendment protected activity. Two were photographing sites of aesthetic interest, one was likely viewing a website about video games inside his home, one was buying computers at Best Buy, and another was standing outside a restroom at a train station while waiting for his mother. Due to the standards issued by Defendants that govern the reporting of information about people supposedly involved in terrorism, Plaintiffs were reported as having engaged in "suspicious activities," reports about them were entered into counterterrorism databases, and they were subjected to unwelcome and unwarranted law enforcement scrutiny and interrogation. Defendants' unlawful standards for maintaining a federal law enforcement database regarding such supposedly "suspicious" activities have not yielded any demonstrable benefit in the fight against terrorism, but they have swept up innocent Americans in violation of federal law.

2. Through the National Suspicious Activity Reporting Initiative ("NSI"), the federal government encourages state and local law enforcement agencies as well as private actors to collect and report information that has a potential nexus to terrorism in the form of so-called Suspicious Activity Reports ("SARs"). SARs are collected and maintained in various counterterrorism databases and disseminated to law enforcement agencies across the country. An individual who is reported in a SAR is flagged as a person with a potential nexus to terrorism and automatically falls under law enforcement scrutiny, which may include intrusive questioning by local or federal law enforcement agents. Even when the Federal Bureau of Investigation concludes that the person did not have any nexus to terrorism, a SAR can haunt that individual for decades, as SARs remain in federal databases for up to 30 years.

3. Defendants Department of Justice ("DOJ") and Program Manager of the Information Sharing Environment ("PM-ISE") have issued standards governing the types of

information that should be reported in a SAR. Both standards authorize the collection, maintenance, and dissemination of information, in the absence of any reasonable suspicion of criminal activity. Defendants have also identified specific categories of behavior that they claim satisfy each agency's standard and should be reported as suspicious. These behavioral categories range from the constitutionally protected (photographing infrastructure) to the absurd ("acting suspiciously").

4. Defendants' standards conflict with a duly promulgated regulation of Defendant DOJ that prohibits the collection, maintenance, and dissemination of criminal intelligence information, unless there is reasonable suspicion of criminal activity. *See* 28 C.F.R. § 23 (1993). The regulation's reasonable suspicion requirement reflects the constitutional principle that law enforcement should not take action against someone, unless there is good reason to believe criminal activity is afoot. Neither of Defendants' standards for reporting suspicious activity was promulgated in accordance with the notice and comment requirements of the Administrative Procedure Act ("APA"), 5 U.S.C. § 551 *et seq*. (2012). As a result, Defendants' issuance and implementation of standards for suspicious activity reporting violate federal statutory requirements that agencies not act in an arbitrary and capricious manner and observe the procedures required by law. Through this action for declaratory and injunctive relief, Plaintiffs seek to set aside as unlawful Defendants' standards for suspicious activity reporting.

PARTIES

5. Plaintiff Wiley Gill is a United States citizen and a custodian at California State University, Chico ("Chico State"). Mr. Gill converted to Islam while he was a student at Chico State. He resides in Chico, California. He is the subject of a SAR, attached as Appendix A to this Complaint. The SAR was uploaded to eGuardian, a law enforcement database maintained by the FBI. The SAR identifies Mr. Gill as a "Suspicious Male Subject in Possession of Flight Simulator Game." Mr. Gill was likely viewing a website about video games on his computer at home, when two officers of the Chico Police Department entered and searched his home without voluntary consent or a warrant based on probable cause.

6. Plaintiff James Prigoff is a United States citizen and an internationally renowned photographer of public art. Mr. Prigoff resides in Sacramento, California. Private security guards warned Mr. Prigoff not to photograph a piece of public art called the "Rainbow Swash" in Boston, Massachusetts. As a result of that encounter, an agent of the Federal Bureau of Investigation ("FBI") went to Mr. Prigoff's home in Sacramento several months later and questioned at least one neighbor about him. Upon information and belief, Mr. Prigoff is the subject of a SAR or SAR precursor report.

7. Plaintiff Khaled Ibrahim is a United States citizen of Egyptian descent who works as an accountant for Nordix Computer Corporation, a computer network consulting and service company. He formerly worked as a purchasing agent for Nordix. Mr. Ibrahim resides in San Jose, California. Mr. Ibrahim is the subject of a SAR, attached as Appendix B to the Complaint. The SAR describes a "[s]uspicious attempt to purchase large number of computers." Mr. Ibrahim attempted to make a bulk purchase of computers from a Best Buy retail store in Dublin, California, in his capacity as a purchasing agent for Nordix. The SAR was uploaded to eGuardian, a law enforcement database maintained by the FBI. Dublin is located in Alameda County, California.

8. Plaintiff Tariq Razak is a United States citizen of Pakistani descent. A graduate of the University of California at Irvine, he works in the bio-tech industry. Mr. Razak resides in Placentia, California. Mr. Razak is the subject of a SAR, attached as Appendix C to this Complaint. The SAR identifies Mr. Razak as a "Male of Middle Eastern decent [sic] observed surveying entry/exit points" at the Santa Ana Train Depot and describes him as exiting the facility with "a female wearing a white burka head dress." Mr. Razak had never been to the Depot before and was finding his way to the county employment resource center, which is located inside the Depot and where he had an appointment. The woman accompanying him was his mother.

9. Plaintiff Aaron Conklin is a graphic design student and amateur photographer. He resides in Vallejo, California. Private security guards have twice prevented Mr. Conklin from taking photographs of industrial architecture from public locations. One such incident

occurred outside the Shell refinery in Martinez, California, and resulted in Mr. Conklin being detained and having his camera and car searched by Contra Costa County Sheriff's Deputies, who told Mr. Conklin that he would be placed on an "NSA watchlist." Upon information and belief, Mr. Conklin is the subject of a SAR. Martinez is located in Contra Costa County, California.

10. Defendant DOJ is a federal agency within the meaning of the APA, 5 U.S.C. § 551(1). DOJ, through its components, has issued a standard governing SAR reporting, conducts trainings on that standard, and plays a major role in implementing the NSI.

11. The FBI is a component of DOJ with both intelligence and law enforcement responsibilities. The FBI has issued a standard governing the reporting of SARs, and trains law enforcement and private sector personnel on its SAR reporting standard. The FBI oversees and maintains the eGuardian system, which serves as a repository for SARs and allows thousands of law enforcement personnel and analysts across the country to access SARs in the eGuardian system. The FBI is one of the primary entities responsible for the NSI.

12. The Office of Justice Programs ("OJP") was created pursuant to 42 U.S.C. § 3711 (2012) and is a component of Defendant DOJ. OJP administers grants to state and local law enforcement entities. Upon information and belief, OJP funding supports, among other things, entities that engage in the collection, maintenance, and dissemination of SARs, and systems that collect, maintain, and disseminate SARs.

13. The Bureau of Justice Assistance ("BJA"), within OJP, provides assistance to local criminal justice programs through policy, programming, and planning. BJA served as the executive agent of the NSI until October 2013. BJA has issued a standard governing the reporting of SARs, and conducts trainings on its SAR reporting standard.

14. The Program Management Office ("PMO"), also a component of DOJ, has played a key role in implementing the NSI. On December 17, 2009, DOJ was named the executive agent to establish and operate the PMO for the NSI. In March 2010, DOJ established the NSI PMO within BJA to support nationwide implementation of the SAR process.

15. Defendant Eric Holder is the Attorney General of the United States and as the head of DOJ is responsible for the regulations, guidelines, and standards adopted by DOJ. He is sued in his official capacity.

16. Defendant PM-ISE is a federal agency within the meaning of the APA, 5 U.S.C. § 551(1) (2012). Pursuant to the Intelligence Reform and Terrorism Prevention Act of 2004 ("IRTPA"), PM-ISE is charged with issuing uniform standards for sharing terrorism and homeland security information across federal, state, and local governments. 6 U.S.C. § 485 (2012). PM-ISE has issued a standard governing SAR reporting and conducts trainings on that standard. PM-ISE's standard for SAR reporting is set forth in "Information Sharing Environment (ISE) - Functional Standard (FS) - Suspicious Activity Reporting (SAR) Version 1.5" ("Functional Standard 1.5"), which the agency issued in May 2009. Functional Standard 1.5 is attached as Appendix D to this Complaint.

17. Defendant Kshemendra Paul occupies the office of the PM-ISE, is the head of PM-ISE, and is responsible for the regulations, guidelines, and standards adopted by PM-ISE. He is sued in his official capacity.

JURISDICTION AND VENUE

18. This is an action under the APA, to set aside agency actions because they are arbitrary and capricious, an abuse of discretion, and not in accordance with law, and because they are without observance of procedure required by law. *See* 5 U.S.C. § 706 (2)(A), (D) (2012). This Court has subject matter jurisdiction pursuant to 28 U.S.C. § 1331 and § 1349 (2012).

19. The Court has authority to grant declaratory relief pursuant to the Declaratory Judgment Act, 28 U.S.C. § 2201 and § 2202 (2012).

20. Venue is proper in this district pursuant to 28 U.S.C. § 1391(e) (2012) because Defendants are agencies of the United States and officers of the United States sued in their official capacities, a substantial part of the events or omissions giving rise to this action occurred in this district, including Alameda and Contra Costa Counties, and one or more plaintiffs reside in this district.

INTRADISTRICT ASSIGNMENT

21. Pursuant to Local Rule 3-2(c) and (d), assignment to the San Francisco-Oakland Division is proper because a substantial part of the events giving rise to this action occurred in Alameda and Contra Costa Counties.

FACTUAL ALLEGATIONS

A. The Nationwide Suspicious Activity Reporting Initiative

22. The federal government created the NSI to facilitate the sharing of information potentially related to terrorism across federal, state, local, and tribal law enforcement agencies. In particular, the NSI creates the capability to share reports of information with a potential nexus to terrorism, which have been dubbed Suspicious Activity Reports.

23. Fusion centers are focal points of the system for sharing SARs. There are currently 78 fusion centers nationwide. They are generally, though not always, owned and operated by state or local government entities. Fusion centers receive federal financial support, including from OJP.

24. Defendants PM-ISE and DOJ train state, local, and tribal law enforcement agencies as well as private entities to collect information about activities with a potential nexus to terrorism based on the standard each agency has adopted, and to submit the information in the form of a SAR, either to a fusion center or the FBI.

25. Fusion centers gather, receive, store, analyze, and share terrorism and other threat-related information, including SARs. On information and belief, fusion centers collect, maintain, and disseminate SARs through databases that receive financial support from OJP.

26. Defendants train fusion center analysts in their respective standards for SAR reporting. Fusion center analysts review submitted SARs. If a SAR meets Defendants' standards, it is uploaded to one or more national databases, such as the FBI's eGuardian system, where it can be accessed by the FBI and law enforcement agencies across the country. The federal government maintains SARs sent to the FBI's eGuardian system for 30 years. This is done even when the FBI determines that the SAR has no nexus to terrorism. *See* Functional Standard 1.5 at 34, 53; United States Government Accountability Office, "Information Sharing:

Additional Actions Could Help Ensure That Efforts to Share Terrorism-Related Suspicious Activity Reports Are Effective" at 7 (March 2013) ("GAO SAR Report").

27. Pursuant to the process created by Defendants PM-ISE and DOJ for suspicious activity reporting, individuals who are the subject of a SAR are automatically subjected to law enforcement scrutiny at multiple levels of government. That scrutiny may include, but is not limited to, follow-up interviews and other forms of investigation by law enforcement. For example:

(a) At the initial response and investigation stage, and even before a SAR is submitted to a fusion center or the FBI, Defendant PM-ISE instructs the federal, state, local, or tribal law enforcement agency with jurisdiction to respond to the reported observation by "gather[ing] additional facts through personal observations, interviews, and other investigative activities. This may, at the discretion of the [responding] official, require further observation or engaging the suspect in conversation." Functional Standard 1.5 at 32.

(b) Fusion center personnel "tak[e] steps to investigate SARs – such as interviewing the individual engaged in suspicious activity or who witnessed suspicious activity – before providing the SARs to the FBI." GAO SAR Report at 16. Officials from fusion centers do investigative work as part of their vetting process. *Id.* at 17.

(c) The FBI reviews all SARs that it receives from fusion centers for follow-up. That follow-up can take the form of an interview with the subject of the SAR, and includes, but is not limited to, engaging in a threat assessment of or opening an investigation into the subject.

(d) FBI agents have admitted that they are required to follow-up on SARs, even when they know the individual does not pose a threat. For example, a professional freelance photographer in Los Angeles, California who specializes in industrial photography, has twice been interviewed by the FBI after photographing industrial sites. After security guards instructed him not to photograph certain industrial sites in the area of the Port of Long Beach in April 2008, FBI agents visited him at his home to question him about the incident. The FBI contacted him again, after Los Angeles Sheriff's Department personnel interfered with his efforts to photograph another industrial site in approximately December 2009. The FBI agent told the photographer that he knew the photographer did not pose a threat but that because a report had been opened, he was required to follow-up on it.

(e) As explained above, SARs that have been uploaded to a national database can be accessed by law enforcement agencies nationwide. Once uploaded to a national database, the subject of a SAR faces scrutiny and potential investigation by one or more of the law enforcement agencies across the country that has access to the database. That scrutiny is only increasing, as queries of national SAR databases have dramatically jumped in recent years. The number of queries of national SAR databases such as eGuardian has risen from about 2,800 queries as of July 2010 to more than 71,000 queries as of February 2013. *See* GAO SAR Report at 36.

28. This surveillance program has not proven effective in the fight against terrorism. The United States Government Accountability Office ("GAO") has faulted the program for failing to demonstrate *any* results-oriented outcomes, such as arrests, convictions, or thwarted threats, even though tens of thousands of SARs had been deemed sufficiently significant to be uploaded to national SAR databases as of October 2012. *See* GAO SAR Report at 33, 36-38. In 2012, a Senate Subcommittee reviewed a year of similar intelligence reporting from state and local authorities, and identified "dozens of problematic or useless" reports "potentially violating civil liberties protections." United States Senate, Permanent Subcommittee on Investigations, Committee on Homeland Security and Governmental Affairs, "Federal Support for and Involvement in State and Local Fusion Centers," October 3, 2012 at 27. Another report, co-authored by Los Angeles Police Department Deputy Chief Michael Downing, found that SARs have "flooded fusion centers, law enforcement, and other security entities with white noise."

The George Washington University Homeland Security Policy Institute, "Counterterrorism Intelligence: Fusion Center Perspectives," June 26, 2012 at 31.

29. While the SARs process has not proven effective in combating terrorism, it has been extremely effective in sweeping up innocent Americans and recording their lawful activity in federal counterterrorism databases. Over 1,800 SARs from fusion centers in California show that the program targets First Amendment protected activity such as photography and encourages racial and religious profiling. Examples of SARs that met Defendants' standards for SAR reporting and have been uploaded to the FBI's eGuardian database include:

- "Suspicious ME [Middle Eastern] Males Buy Several Large Pallets of Water"
- A sergeant from the Elk Grove Police Department reported "on a suspicious individual in his neighborhood"; the sergeant had "long been concerned about a residence in his neighborhood occupied by a Middle Eastern male adult physician who is very unfriendly"
- "Female Subject taking photos of Folsom Post Office"
- "an identified subject was reported to be taking photographs of a bridge crossing the American River Bike trail"
- "I was called out to the above address regarding a male who was taking photographs of the [name of facility blacked out] [in Commerce, California]. The male stated, he is an artist and enjoys photographing building[s] in industrial areas … [and] stated he is a professor at San Diego State private college, and takes the photos for his art class."
- "I observed a male nonchalantly taking numerous pictures inside a purple line train [in Los Angeles County] … The male said he was taking pictures because they were going to film the television show '24' on the train next week."
- "two middle eastern looking males taking photographs of Folsom Dam. One of the ME males appeared to be in his 50's"
- "Suspicious photography of the Federal Courthouse in Sacramento": an "AUSA [Assistant United States Attorney] reported to the Court Security Officer (CSO) a

suspicious vehicle occupied by what [name blacked out] described as two Middle Eastern males, the passenger being between 40-50 years of age."

- "Suspicious photography of Folsom Dam by Chinese Nationals": "a Sac County Sheriff's Deputy contacted 3 adult Asian males who were taking photos of Folsom Dam. They were evasive when the deputy asked them for identification and said their passports were in their vehicle."

B. Conflicting Federal Rules for Collection of Intelligence Information

30. Defendants have issued three separate rules governing the collection of intelligence information, in particular, suspicious activity reports. Only one of these rules, however, requires reasonable suspicion of criminal activity for the information to be collected, maintained, and disseminated, and only that rule was duly promulgated under the APA.

1. 28 C.F.R. Part 23

31. On June 19, 1968, President Lyndon B. Johnson signed into law the Omnibus Crime Control and Safe Streets Act of 1968 ("Omnibus Act"). The Act created the Law Enforcement Administration Agency ("LEAA"), a forerunner to OJP and a component of DOJ, and authorized it to oversee the distribution of federal grants to state and local law enforcement programs.

32. In 1978, after observing the notice and comment process set forth in the APA, Defendant DOJ, through its component the LEAA, published a final rule establishing operating principles for "Criminal Intelligence Systems." *See* 28 C.F.R. § 23 (1993). The regulation was promulgated pursuant to the LEAA's statutory mandate to ensure that criminal intelligence is not collected, maintained, or disseminated "in violation of the privacy and constitutional rights of individuals." 42 U.S.C. § 3789g(c) (2012).

33. Several commenters on the then-proposed regulation "were concerned that the collection and maintenance of intelligence information should only be triggered by a reasonable suspicion that an individual is involved in criminal activity." *See* 43 Fed. Reg. 28,572 (June 30, 1978). The agency concurred, and the proposed operating principles were "revised to require this criteria as a basis for collection and maintenance of intelligence information." *Id.*

34. Among other requirements, the final rule provides that a "project shall collect and maintain criminal intelligence information concerning an individual only if there is reasonable suspicion that the individual is involved in criminal conduct or activity and the information is relevant to that criminal conduct or activity." 28 CFR § 23.20(a).

35. In addition, the regulation states that while "pooling of information about" various kinds of criminal activities such as drug trafficking, smuggling, and public corruption can be helpful in "expos[ing] … ongoing networks of criminal activity," "the collection and exchange of intelligence data necessary to support control of serious criminal activity may represent potential threats to the privacy of individuals to whom such data relates," and the privacy guidelines set forth in 28 CFR Part 23 are therefore necessary. 28 CFR § 23.2.

36. In 1980, DOJ amended the rule, following the public notice and comment process set forth in the APA, to extend the reach of 28 C.F.R. Part 23 to criminal intelligence systems funded by both discretionary and formula grants. 45 Fed. Reg. 61,612 (Sep. 17, 1980).

37. DOJ amended the rule again in 1993 to include a definition of "reasonable suspicion":

> Reasonable Suspicion . . . is established when information exists which establishes sufficient facts to give a trained law enforcement or criminal investigative agency officer, investigator, or employee a basis to believe that there is a reasonable possibility that an individual or organization is involved in a definable criminal activity or enterprise.

See 28 C.F.R. § 23.20.

38. "Reasonable suspicion" is the time-tested, constitutional standard that limits law enforcement from taking action against someone, unless there is good reason to believe criminal activity is afoot.

39. One commenter argued that "reasonable suspicion . . . is not necessary to the protection of individual privacy and Constitutional rights, [and suggested] instead that information in a funded intelligence system need only be 'necessary and relevant to an agency's lawful purposes.'" 58 Fed. Reg. 178, 48451 (Sept. 16, 1993). The agency disagreed, replying:

> the potential for national dissemination of information in intelligence information systems, coupled with the lack of access by subjects to challenge the information, justifies the reasonable suspicion standard as well as other operating principle restrictions set forth in this regulation. Also, the quality and utility of 'hits' in an information system

> is enhanced by the reasonable suspicion requirement. Scarce resources are not wasted by agencies in coordinating information on subjects for whom information is vague, incomplete and conjectural.

Id.

40. DOJ made an attempt in 2008 to amend the regulation to weaken its privacy protections. In particular, the proposed rule would have (1) permitted information to be stored regarding organizations as well as individuals; (2) allowed information to be stored based on reasonable suspicion related to "domestic and international terrorism, including material support thereof," and (3) eliminated the requirement that law enforcement agencies receiving information from a Criminal Intelligence System agree to comply with 28 C.F.R. Part 23, so that recipients would merely need to have procedures "consistent with" Section 23. *See* 73 Fed. Reg. 44,674 (July 31, 2008). This attempted rulemaking, however, met with criticism and DOJ withdrew its proposed rule. The regulation has remained unchanged since its last amendment in 1993.

41. In short, in initially adopting the regulation, DOJ emphasized the importance of the reasonable suspicion requirement and since then has expanded the scope of the regulation, reiterated the importance of the reasonable suspicion requirement, and withdrawn efforts to weaken the regulation's privacy protections.

2. PM-ISE Standard for Suspicious Activity Reporting

42. Defendant PM-ISE subsequently issued a standard for SAR reporting that – unlike 28 CFR Part 23 – does not require reasonable suspicion of criminal activity before a suspicious activity report is collected, maintained, or disseminated and was not issued through the notice and comment procedure required by the APA, thus dodging public review.

43. Pursuant to the exercise of its statutory authority to "exercise governmentwide authority over the sharing of [terrorism and homeland security] information," 6 U.S.C. § 485(f)(1) (2012), PM-ISE has issued "Functional Standards" governing suspicious activity reporting.

44. In or about May 2009, PM-ISE released Information Sharing Environment (ISE) - Functional Standard (FS) - Suspicious Activity Reporting (SAR) Version 1.5 ("Functional Standard 1.5"), which remains currently in effect. It sets forth the following standard for

suspicious activity reporting: "[o]bserved behavior *reasonably indicative* of pre-operational planning related to terrorism or other criminal activity." Functional Standard 1.5 at 2 (emphasis added).

45. The agency has expressly acknowledged that Functional Standard 1.5 requires "less than the 'reasonable suspicion' standard." PM-ISE, Privacy, Civil Rights, and Civil Liberties Analysis and Recommendations–Nationwide Suspicious Activity Reporting Initiative at 12 (draft May 2010).

46. The document also identifies sixteen categories of activity that fall under the standard and provide a guide to law enforcement in determining what amounts to a suspicious activity. These categories include photography, observation/surveillance, and acquisition of materials or expertise. Functional Standard 1.5 at 29-30.

47. Functional Standard 1.5 applies to, *inter alia*, "all departments or agencies that possess or use terrorism or homeland security information." Functional Standard 1.5 at 1. Functional Standard 1.5 applies to state, local, and tribal law enforcement agencies and fusion centers that participate in the NSI. Agencies participating in the NSI follow Functional Standard 1.5 in reporting suspicious activity.

48. Functional Standard 1.5 purports to define the scope of suspicious activity that should be reported for agencies participating in the NSI. The purpose of Functional Standard 1.5 is to standardize SAR reporting at the federal, state, and local levels.

49. PM-ISE trains participants in the NSI about, among other things, how to follow Functional Standard 1.5.

50. In promulgating Functional Standard 1.5, PM-ISE expressly cited its legislative authority under, *inter alia*, the IRTPA over governmentwide standards for information sharing. Functional Standard 1.5 at 1.

51. Functional Standard 1.5 constitutes final agency action and a legislative rule within the meaning of the APA.

52. PM-ISE issued Functional Standard 1.5 without observing the process set forth in the APA for public notice and comment. Functional Standard 1.5 went into immediate effect upon its publication on May 1, 2009 and remains currently in effect.

3. DOJ Standard for Suspicious Activity Reporting

53. Defendant DOJ, through its components, has issued a standard for SAR reporting ("DOJ's SAR Standard") that – unlike 28 CFR § 23 – does not require reasonable suspicion of criminal activity before a suspicious activity report is collected, maintained, or disseminated and was not issued through the notice and comment procedure required by the APA, thus dodging public review.

54. DOJ, through its component the FBI, has set forth the following standard for suspicious activity reporting: "observed behavior that *may be indicative* of intelligence gathering or pre-operational planning related to terrorism, criminal or other illicit intention." FBI, Privacy Impact Assessment for the eGuardian Threat Tracking System at § 1.1 (emphasis added). This standard is set forth in the FBI's 2008 eGuardian Privacy Impact Assessment ("2008 eGuardian PIA"), which is attached as Appendix E to this Complaint. "[T]he FBI uses the criteria in the eGuardian Privacy Impact Assessment (dated November 25, 2008) … to determine if SARs have a potential nexus to terrorism." GAO SAR Report at 6 n.10.

55. DOJ's "may be indicative" SAR Standard is even broader than PM-ISE's "reasonably indicative" Functional Standard 1.5. *See* GAO SAR Report at 15-16. But like Functional Standard 1.5, DOJ's SAR Standard encourages reporting even in the absence of reasonable suspicion of criminal activity.

56. Just as Defendant PM-ISE has enumerated categories of behavior that fall under its "reasonably indicative" reporting standard, DOJ through its components has also enumerated categories of behavior that fall under its "may be indicative" reporting standard. These categories of behavior are broader than the categories set forth in Functional Standard 1.5 and include but are not limited to:

(a) "Possible indicators of terrorist behaviors at hotels:…" FBI and United States Department of Homeland Security, "Roll Call Release," July 26, 2010, attached as Appendix F to this Complaint.

(1) "Using payphones for outgoing calls or making front desk requests in person to avoid using the room telephone." *Id.*

(2) "Interest in using Internet cafes, despite hotel Internet availability…." *Id.*

(3) "Requests for specific rooms, floors, or other locations in the hotel…." *Id.*

(4) "Multiple visitors or deliveries to one individual or room." *Id.*

(b) "No obvious signs of employment." FBI, "Quick Reference Terrorism Card," attached as Appendix G to this Complaint.

(c) "Possess student visa but not English Proficient." *Id.*

(d) "Persons not fitting into the surrounding environment, such as wearing improper attire for the location." *Id.*

(e) "Persons exhibiting unusual behavior such as staring or quickly looking away from individuals or vehicles as they enter or leave designated facilities or parking areas." *Id.*

(f) "A blank facial expression in an individual may be indicative of someone concentrating on something not related to what they appear to be doing." *Id.*

(g) "[P]eople in places where they do not belong." Bureau of Justice Assistance, "Communities Against Terrorism: Potential Indicators of Terrorist Activities Related to the General Public," attached as Appendix H to this Complaint.

57. One category of behavior identified by DOJ as "suspicious" activity that should be reported is a "catch-all":

(a) "[P]eople acting suspiciously." *Id.*

58. DOJ through its components has also issued "Potential Indicators of Terrorist Activities Related to Electronic Stores" (attached as Appendix I to this Complaint) and

"Potential Indicators of Terrorist Activities Related to Mass Transportation" (attached as Appendix J to this Complaint). Activities identified as suspicious in connection with mass transportation include "[a]cting nervous or suspicious," and "[u]nusual or prolonged interest in … entry points and access controls."

59. DOJ through its components trains participants in the NSI about DOJ's SAR Standard. For example, as of 2013, the PMO had provided training for 290,000 line officers (law enforcement officers whose routine duties put them in a position to observe "suspicious" activity), 2,000 analytical personnel, and executives from 77 fusion centers. *See* GAO SAR Report at 29. DOJ components teach participants in the NSI, including frontline officers and fusion center analysts to submit to the FBI "all potentially terrorism-related information and not just ISE-SARs that met the [PM-ISE's] Functional Standard [1.5]." GAO SAR Report at 16.

60. DOJ's SAR Standard applies to state, local, and tribal law enforcement agencies and fusion centers that participate in the NSI. Agencies participating in the NSI follow DOJ's SAR Standard in reporting suspicious activity.

61. DOJ's SAR Standard purports to define the scope of suspicious activity that should be reported for agencies participating in the NSI. The purpose of DOJ's SAR Standard is to standardize SAR reporting at the federal, state, and local levels.

62. Because DOJ's SAR Standard is broader than PM-ISE's Functional Standard 1.5 and DOJ's behavioral categories include the catch-all "people acting suspiciously," any activity that falls under PM-ISE's Functional Standard also falls under DOJ's SAR Standard.

63. Fusion centers that follow DOJ's SAR Standard instead of PM-ISE's Functional Standard 1.5 send many SARs to the FBI for review. For example, of the SARs uploaded by one state's fusion center to a national SAR database from June 2011 to October 2012, only 10% met PM-ISE's Functional Standard 1.5. *See* GAO SAR Report at 16.

64. DOJ establishes an even broader standard than the already overbroad Functional Standard 1.5, and the DOJ reinforces its broader standard through the trainings it provides to NSI participants and through other mechanisms. For example, when fusion center personnel are uncertain whether to share a SAR, DOJ encourages them to err on the side of overreporting. *See*

GAO SAR Report at 16. In addition, the only feedback mechanism participants in the NSI currently receive on whether they are reporting SARs appropriately is provided by the FBI through its eGuardian system. *See* GAO SAR Report at 13-14. The feedback the FBI provides reinforces the DOJ SAR Standard to NSI participants.

65. DOJ's 2008 eGuardian PIA, which sets forth the agency's standard for reporting suspicious activity, was signed by four "Responsible Officials," two "Reviewing Officials," and one "Approving Official." It reflects the consummation of the agency's decision making process.

66. DOJ's 2008 eGuardian PIA contains a set of mandatory, non-discretionary rules and obligations. It lays out clear instructions for the use of the eGuardian system to collect and share SARs and the standard for defining "suspicious activity." For example, the 2008 eGuardian PIA states that the eGuardian system will "ensure consistency of process and of handling protocols" and mandates that all users "will be required to complete robust system training that will incorporate eGuardian policies and procedures." 2008 eGuardian PIA at 4. In addition, the eGuardian User Agreement, attached to the 2008 eGuardian PIA, states that "[i]ncidents not meeting the criteria of suspicious activity or with a potential nexus to terrorism and that, further, do not comply with the above-stated rules, will be immediately deleted from eGuardian." 2008 eGuardian PIA at 25.

67. DOJ has consistently reinforced its standard for SAR reporting, set forth in the 2008 eGuardian PIA, through training materials and other publications that identify categories of behavior that the agency contends are suspicious and should be reported.

68. In promulgating DOJ's SAR Standard, DOJ expressly invoked its statutory "mandate" under IRTPA and "other statutes … to share terrorism information with other federal, and state, local and tribal (SLT) law enforcement partners." 2008 eGuardian PIA at 2.

69. DOJ's SAR Standard constitutes final agency action and a legislative rule within the meaning of the APA.

70. Defendant DOJ issued the DOJ SAR Standard without observing the process set forth in the APA for public notice and comment. It is the DOJ Standard for SAR reporting currently in effect.

4. PM-ISE's Functional Standard 1.5 and DOJ's SAR Standard Conflict with 28 CFR Part 23

71. As a report of "[o]bserved behavior reasonably indicative of pre-operational planning related to terrorism or other criminal activity" (Functional Standard 1.5) or a report of "observed behavior that may be indicative of intelligence gathering or pre-operational planning related to terrorism, criminal or other illicit intention" (DOJ's SAR Standard), a SAR contains data relevant to the identification of an individual who is suspected in some fashion of being involved in criminal, in particular, terrorist activity.

72. A SAR constitutes "criminal intelligence" within the meaning of 28 CFR Part 23.

73. State, local, and tribal law enforcement agencies and fusion centers that participate in the NSI and observe PM-ISE's Functional Standard 1.5 and/or DOJ's SAR Standard collect, review, analyze, and disseminate SARs. These entities operate arrangements, equipment, facilities, and procedures, used for the receipt, storage, interagency exchange or dissemination, and analysis of SARs. Upon information and belief, these entities and the systems they operate for receiving, storing, exchanging, disseminating, and analyzing SARs operate through support from Defendant DOJ's component OJP.

74. State, local, and tribal law enforcement agencies and fusion centers that participate in the NSI and observe PM-ISE's Functional Standard 1.5 and/or DOJ's SAR Standard are "projects" within the meaning of 28 CFR Part 23. The systems or databases on which SARs are maintained and through which they are collected and disseminated are "criminal intelligence systems" within the meaning of 28 CFR Part 23.

75. PM-ISE's Functional Standard 1.5 and DOJ's SAR Standard set forth operating principles for the collection, maintenance, and dissemination of data relevant to the identification of an individual who is suspected in some fashion of being involved in criminal, in particular, terrorist activity. Both standards, however, encourage or purport to authorize collection,

maintenance, and dissemination of such data even in the absence of reasonable suspicion of criminal activity. Both standards encourage or purport to authorize collection, maintenance, and dissemination of much more data than that permitted under 28 CFR Part 23. Both standards therefore conflict with 28 CFR Part 23.

76. Through PM-ISE's promulgation of Functional Standard 1.5 and DOJ's promulgation of its SAR Standard, and through each agency's training of entities participating in the NSI in their respective standards for reporting suspicious activity, Defendants PM-ISE, Paul, DOJ, and Holder have undermined and thereby violated 28 CFR Part 23.

77. Neither DOJ nor PM-ISE has offered any reasoned basis for departing from the reasonable suspicion standard set forth in 28 CFR Part 23 for the collection, maintenance, and dissemination of SARs.

78. DOJ could rescind its SAR reporting standard. If DOJ rescinded its SAR reporting standard, participants in the NSI would cease collecting, maintaining, reviewing, analyzing and disseminating SARs based on DOJ's SAR Standard, and it would be clear that the governing standard for suspicious activity reporting is 28 CFR Part 23. As a result, individuals who are currently the subject of SARs but whose conduct did not give rise to a reasonable suspicion of criminal activity would no longer have their information collected, maintained, and disseminated in SAR databases. DOJ could cease collecting, maintaining, reviewing, analyzing, and disseminating SARs about individuals whose conduct did not give rise to a reasonable suspicion of criminal activity.

79. PM-ISE could rescind Functional Standard 1.5. If PM-ISE rescinded Functional Standard 1.5, participants in the NSI would cease collecting, maintaining, reviewing, analyzing and disseminating SARs based on Functional Standard 1.5, and it would be clear that the governing standard for suspicious activity reporting is 28 CFR Part 23. As a result, individuals who are currently the subject of SARs but whose conduct did not give rise to a reasonable suspicion of criminal activity would no longer have their information collected, maintained, and disseminated in SAR databases.

C. Plaintiff's Allegations

1. Wiley Gill

80. Wiley Gill is a United States citizen living in Chico, California. He works as a custodian at Chico State, which he attended as an undergraduate. Mr. Gill converted to Islam in 2009, after learning about the religion in a course he took while a student at Chico State.

81. Mr. Gill is the subject of a SAR that identifies him as a "Suspicious Male Subject in Possession of Flight Simulator Game." This SAR falls into one or more of the behavioral categories identified in Functional Standard 1.5, in particular, "[a]cquisition of [e]xpertise" and potentially "[a]viation [a]ctivity." Functional Standard 1.5 at 29-30. It also falls under one or more behavioral categories identified by Defendant DOJ, such as the catch-all behavioral category of "acting suspiciously."

82. Mr. Gill's SAR was collected, maintained, and disseminated through a fusion center SAR database, and uploaded to eGuardian and/or another national SAR database. As a result, the FBI has scrutinized Mr. Gill, conducted extensive background checks on him, and created a file about him.

83. The SAR was created on or about May 23, 2012, and purports to document an encounter between Mr. Gill and the Chico Police Department ("CPD") on or about May 20, 2012. The SAR states that a CPD officer was investigating a domestic violence incident and believed the suspect may have fled into Mr. Gill's residence. The SAR states that this was later discovered to be unfounded. It acknowledges that the CPD officer searched Mr. Gill's home. The SAR asserts that Mr. Gill's computer displayed a screen titled something to the effect of "Games that fly under the radar," which appeared to be a "flight simulator type of game." The SAR concludes by describing Mr. Gill's "full conversion to Islam as a young WMA [white, male adult]," "pious demeanor," and "potential access to flight simulators via the internet" as "worthy of note."

84. CPD's search of Mr. Gill's residence on or about May 20, 2012 did in fact occur. But the SAR contains numerous misstatements and omits several crucial facts, including that two CPD officers banged on Mr. Gill's door and after when he went to open it, they came around the

corner of the house with their guns drawn and pointed at Mr. Gill. Mr. Gill was thrown off guard. The officers eventually lowered their guns, and then asked to search Mr. Gill's home, based on the alleged domestic violence incident involving two individuals that they claimed to have received. Mr. Gill informed the officers that he was home alone. Despite that, the officers continued to ask to search his home. Mr. Gill was reluctant to grant permission, but felt that he had no choice under the circumstances. One officer remained with Mr. Gill outside, while the other searched his home. Mr. Gill did not feel free to leave. Mr. Gill cooperated with the officers' request for identification. Mr. Gill believes that he was likely viewing a website about video games at the time of the May 20, 2012, incident.

85. On information and belief, the officers' contention that they were investigating a domestic violence call was a pretext for searching Mr. Gill's home because CPD had already decided to investigate Mr. Gill because of his religion.

86. The SAR also describes two earlier encounters between CPD and Mr. Gill, one at the Mosque that Mr. Gill attends and another while Mr. Gill was walking through downtown Chico "with elders." The SAR describes Mr. Gill in these instances as "avoid[ing] eye contact" and "hesitant to answer questions."

87. Mr. Gill recalls CPD officers visiting the Mosque he attends, paying what they described as a courtesy visit in an attempt to build good relations with the Muslim community. Mr. Gill listened to the presentation. When it was over, CPD officers asked Mr. Gill his name, whether he went to school, and if he was employed. Mr. Gill answered all of their questions. His understanding is that the officers did not question anyone else in this manner.

88. Mr. Gill also recalls encountering CPD officers while he was walking through downtown Chico with two older Muslim men who are friends from the Mosque. A CPD officer called out Mr. Gill's name and asked Mr. Gill if he had found a job yet. Mr. Gill answered the question, but was caught off guard by the encounter because he did not recognize the officer and was surprised that the officer knew his name and employment status.

89. At no point during any of the encounters with CPD recounted in the SAR did Mr. Gill engage in conduct that gave rise to a reasonable suspicion of criminal activity.

90. The CPD also targeted Mr. Gill in two other encounters that are not described in the SAR, and that do not involve any conduct by Mr. Gill that gave rise to a reasonable suspicion of criminal activity, but instead reflect CPD's suspicion of Mr. Gill because of his religion. One of the incidents occurred before CPD filed the SAR about Mr. Gill on or about May 23, 2012; the other occurred after. This religious harassment is attributable to the training of local law enforcement on the SARs standards and process.

91. In approximately September 2010, after Mr. Gill had converted to Islam, two CPD officers visited him at his apartment and requested to speak to him about supposedly "anti-American statements" that he had made. One of the officers referred to having a file on Mr. Gill, refused to explain what "anti-American statements" Mr. Gill had purportedly made or the source of the information, and stated that he wished to ensure Mr. Gill would not turn into another Mohammed Atta, one of the individuals identified as a September 11 hijacker. Mr. Gill still does not know how he came to the attention of the CPD.

92. Around or after July 2012, Mr. Gill also received a telephone call from a CPD officer. Over the phone, the CPD officer said Mr. Gill should shut down his Facebook page because of the video games Mr. Gill played. At the time, Mr. Gill had a picture of the Shahada, the Muslim statement of faith, on his Facebook page. Mr. Gill told the CPD officer he would not take down his Facebook page and Mr. Gill also told the CPD officer that he believed the CPD wanted Mr. Gill to take down his Facebook page because of its references to Islam. The CPD officer refused to comment on Mr. Gill's observation, but stated that he had a report on Mr. Gill and indicated that Mr. Gill was on some kind of watch list.

93. By describing Mr. Gill's conversion to Islam and "pious demeanor" in the SAR as "worthy of note," CPD implicitly acknowledges that it found him "suspicious" because he is a devout Muslim.

94. Defendants' issuance of overly broad definitions of "suspicious activity" and the categories of behavior they have identified as "suspicious" include, among other things, "[a]cquisition of expertise" (PM-ISE) and "[n]o obvious signs of employment" (DOJ). On information and belief, CPD officers are trained in Defendants' standards for SAR reporting.

95. Defendants' overly broad standards for reporting suspicious activity opens the door to and encourages religious profiling. These standards opened the door to and encouraged the religious profiling of Mr. Gill by CPD, CPD's repeated questioning and ongoing scrutiny of Mr. Gill, and CPD's identification of Mr. Gill in a SAR as someone engaged in activity with a potential nexus to terrorism.

96. In addition, Functional Standard 1.5 instructs law enforcement agencies at the "[i]nitial [r]esponse and [i]nvestigation stage" to respond to the observation reported in a SAR, and "gather[] additional facts," by, *inter alia*, "engaging the suspect in conversation" and "other investigative activities." Functional Standard 1.5 at 32. The CPD was implementing the protocols set forth in Functional Standard 1.5 when it harassed Mr. Gill on or about May 2012, before, and after.

97. Because Mr. Gill is the subject of a SAR that falls under Defendants' standards for suspicious activity reporting, Mr. Gill has been automatically subjected to law enforcement scrutiny. That scrutiny has included, among other things, CPD's telephone call to him around or after July 2012 and the FBI's creation of a file about and investigation of Mr. Gill.

98. Given the repeated harassment Mr. Gill has already suffered by CPD, he fears further action may be taken against him by CPD and other investigative agencies as the result of this SAR. He also fears further investigative harassment at the hands of the CPD and other agencies caused by the existence of the SAR.

99. Mr. Gill also has experienced frustration and stress resulting from the creation of the SAR based on innocent conduct. He is also deeply troubled by what may result from the collection, maintenance, and dissemination in a national database of a report describing him as engaging in suspicious activity with a potential nexus to terrorism.

100. The SAR about Mr. Gill is maintained and will continue to be maintained in one or more national SAR databases, where it can be accessed by law enforcement agencies across the country.

//

//

2. James Prigoff

101. James Prigoff is a United States citizen who resides in Sacramento, California. He is an internationally renowned photographer. The focus of his work is public art, such as murals and graffiti art. He has amassed over 80,000 photographic slides and published several books containing his photography. Mr. Prigoff is also a former business executive, having served as a Senior Vice President of the Sara Lee Corporation and a President of a division of Levi Strauss.

102. In or around the spring of 2004, Mr. Prigoff was in Boston, Massachusetts. While there, he sought to photograph a famous piece of public art known as the "Rainbow Swash," located in the Dorchester neighborhood of Boston. The artwork is painted on a natural gas storage tank, which is surrounded by a chain link fence. It is highly visible to commuters from the local expressway.

103. Mr. Prigoff drove a rental car to a public area outside the fence surrounding the Rainbow Swash, and set up to take photographs. He chose the location in part because of favorable lighting conditions. From this location, the sun was behind him and casting its light on the Rainbow Swash. Before Mr. Prigoff could take any photographs, two private security guards came out from inside the fenced area and told him that he was not allowed to photograph, claiming the area was private property. Mr. Prigoff pointed out to the security guards that he was not, in fact, on private property. The guards still insisted that Mr. Prigoff could not photograph.

104. To avoid a confrontation with the guards, Mr. Prigoff departed. He left without giving the security guards any identifying information.

105. He drove further down the road to another public location outside the fenced perimeter and attempted to take photographs from this second location. But the guards began to follow him.

106. To avoid further harassment by the guards, he drove to a third location on the other side of the Rainbow Swash. The guards did not follow him to this third location, and he was finally able to take photographs of the Rainbow Swash unmolested. But the lighting

conditions were significantly inferior to those at the first two locations; from this third location, he had to photograph into the sunlight.

107. At no point while he was attempting to photograph the Rainbow Swash did Mr. Prigoff engage in conduct that gave rise to a reasonable suspicion of criminal activity.

108. Mr. Prigoff subsequently discovered photographs online, including on the Rainbow Swash's Wikipedia webpage. These widely available photographs were taken from vantage points closer than the three locations from which Mr. Prigoff attempted to and actually took photographs.

109. Mr. Prigoff returned to his home in Sacramento, California after his trip to Boston. A few months later, on or about August 19, 2004, he came home one day to find a business card affixed to his door from Agent A. Ayaz of the Joint Terrorism Task Force, which, as noted above, is a partnership between the FBI and other law enforcement agencies. On the back was a handwritten note stating, "Mr. Prigoff, please call me. Thanks." Mr. Prigoff later learned from a neighbor across the street that two agents had knocked on her door and asked for information about Mr. Prigoff.

110. Mr. Prigoff called Mr. Ayaz, who asked if Mr. Prigoff had been to Boston. Realizing that Mr. Ayaz was referring to his efforts to photograph a piece of public art, Mr. Prigoff explained what had occurred. On information and belief, security guards at the site of the Rainbow Swash had submitted a SAR or SAR precursor report regarding Mr. Prigoff that included his rental car information, after which authorities traced him from Boston, Massachusetts, to his home in Sacramento, California.

111. Mr. Prigoff is very upset that he was tracked cross-country from Boston to Sacramento, and contacted by law enforcement agents at his home over his effort to engage in photography from a public location. Mr. Prigoff is also very upset that law enforcement agents questioned at least one of his neighbors about him, as such questioning casts the negative and strong implication that Mr. Prigoff had somehow engaged in misconduct.

112. Taking photographs of infrastructure falls under one or more of the behavioral categories identified by Defendant PM-ISE under Functional Standard 1.5 as "suspicious," and

also falls under one or more behavioral categories identified by Defendant DOJ, such as the catch-all behavioral category of "acting suspiciously." After attempting to photograph a piece of public art painted on a natural gas storage tank in Boston, Mr. Prigoff was tracked to his home in Sacramento and questioned about his trip to Boston, even though he never provided the security guards with identifying information. On information and belief, Mr. Prigoff is the subject of a SAR or SAR precursor report, which was filed by security guards at the Rainbow Swash. On information and belief, the report about him was collected, maintained, and disseminated through a fusion center database, and uploaded to eGuardian and/or another national SAR or similar counterterrorism database. On information and belief, the report about him was collected, maintained, and disseminated under standards that authorized collection, maintenance and dissemination of information even in the absence of reasonable suspicion of criminal activity; Defendants' standards for SAR reporting ratify that conduct.

113. On information and belief, security guards at the Rainbow Swash were trained in standards that encourage reporting of activity deemed connected to terrorism, even in the absence of reasonable suspicion of criminal activity; Defendants' standards for SAR reporting ratify that conduct. Because of that training, they interfered with Mr. Prigoff's lawful efforts to take photographs of the Rainbow Swash.

114. Because Mr. Prigoff is the subject of a report that falls under Defendants' standards for suspicious activity reporting, Mr. Prigoff has been automatically subjected to law enforcement scrutiny. That scrutiny has included but may not be limited to a follow-up visit by an agent of the Joint Terrorism Task Force to his home, a telephone call with that agent, and inquiries by that agent of at least one of his neighbors about him.

115. Upon information and belief, the report about Mr. Prigoff is maintained and will continue to be maintained in one or more national SAR or similar counterterrorism databases, where it can be accessed by law enforcement agencies across the country.

116. Mr. Prigoff continues to be an active photographer and often takes pictures of architectural structures and post offices, among other sites that could be described as "infrastructure." Because taking photographs of infrastructure falls under one or more of the

behavioral categories identified by Defendant PM-ISE under Functional Standard 1.5 as "suspicious," and also falls under one or more behavioral categories identified by Defendant DOJ, such as the catch-all behavioral category of "acting suspiciously," he is likely to be the subject of another SAR in the future. He fears that his efforts to take photographs of such areas will be hindered again in the future.

117. Mr. Prigoff is also deeply troubled by what may result from the collection, maintenance, and dissemination in a national database of a report describing him as engaging in suspicious activity with a potential nexus to terrorism.

3. Khaled Ibrahim

118. Khaled Ibrahim is a United States citizen of Egyptian descent living in San Jose, California. He works in accounting for Nordix Computer Corporation, a computer network consulting and service company. He formerly worked as a purchasing agent for Nordix. As part of his job as purchasing agent, Mr. Ibrahim bought computers in bulk from retail stores, where the stores allowed such transactions.

119. On several occasions in 2011, Mr. Ibrahim went to the Best Buy in Dublin, California in order to attempt to purchase computers in bulk for Nordix. On one such occasion, he was told that management did not allow such bulk purchases and, with that, Mr. Ibrahim left.

120. At no point while he was attempting to purchase computers from Best Buy did Mr. Ibrahim engage in conduct that gave rise to a reasonable suspicion of criminal activity.

121. Mr. Ibrahim is the subject of a SAR, created on November 14, 2011, regarding Mr. Ibrahim's attempts to purchase "a large amount of computers." The SAR about him was collected, maintained, and disseminated through a fusion center SAR database, and uploaded to the FBI's eGuardian database. Upon information and belief, the personnel at the fusion center who uploaded Mr. Ibrahim's SAR to eGuardian were trained in Defendants' standards for SAR reporting.

122. The SAR pertaining to Mr. Ibrahim falls into one or more of the behavioral categories identified in Functional Standard 1.5, in particular, "[a]cquisition … of unusual quantities of materials." Functional Standard 1.5 at 30. It also falls under one or more

behavioral categories identified by Defendant DOJ, such as the catch-all behavioral category of "acting suspiciously" and DOJ's "Potential Indicators of Terrorist Activities Related to Electronic Stores."

123. Because Mr. Ibrahim is the subject of a SAR that falls under Defendants' standards for suspicious activity reporting, Mr. Ibrahim has been automatically subjected to law enforcement scrutiny. That scrutiny may include but is not limited to scrutiny or interviews by any of the law enforcement agencies across the country that have access to the FBI's eGuardian system, to which his SAR was uploaded.

124. Mr. Ibrahim is particularly disturbed that trained law enforcement personnel at a fusion center uploaded the SAR about him to eGuardian, thereby flagging him as an individual with a potential nexus to terrorism. He is also troubled by what may result from the collection, maintenance, and dissemination in a national database of a report describing him as engaging in suspicious activity with a potential nexus to terrorism. Mr. Ibrahim is upset that a SAR was entered about him potentially because of his Middle Eastern descent, and believes that this system of racial profiling diminishes the rights of Middle Eastern communities.

125. The SAR about Mr. Ibrahim is maintained and will continue to be maintained in one or more national SAR databases, where it can be accessed by law enforcement agencies across the country.

4. Tariq Razak

126. Tariq Razak is a United States citizen of Pakistani descent. He resides in Placentia, California. A graduate of the University of California at Irvine, he works in the bio-tech industry.

127. Mr. Razak is the subject of a SAR pertaining to a "Male of Middle Eastern decent [sic] observed surveying entry/exit points" at the Santa Ana Train Depot.

128. On May 16, 2011, Santa Ana Police Officer J. Gallardo filed a SAR regarding Mr. Razak. According to the SAR, Officer Gallardo responded to a call at the Santa Ana Train Depot from Security Officer Karina De La Rosa. Ms. De La Rosa explained that her "suspicion became aroused because the male appeared to be observant of his surroundings and was

constantly surveying all areas of the facility. The male's appearance was neat and clean with a closely cropped beard, short hair wearing blue jeans and a blue plaid shirt." The SAR goes on to describe how Mr. Razak, after studying entry/exit points moved to a part of the train station where the restrooms are located and eventually departed the train station with "a female wearing a white burka head dress" who had emerged from the restrooms. Office Gallardo concludes the SAR by requesting that it be forwarded to the fusion center in Orange County "for review and possible follow-up."

129. According to the SAR, Security Officer De La Rosa stated that "she received 'suspicious activity as related to terrorism training'" and that "the behavior depicted by the male was similar to examples shown in her training raising her suspicion and making the decision to notify the police." Mr. Razak is the subject of the SAR because of Defendants' trainings on their SAR reporting standards to state and local law enforcement and the private sector.

130. Mr. Razak was, indeed, at the Santa Ana Train Depot on May 16, 2011. The woman he was with was his mother. He had an appointment at the county employment resource center, which is located in the station building. He had not been to the station before and spent some time locating the office before meeting up with his mother by the restrooms and leaving. His mother was wearing a hijab (head scarf), and not a burka.

131. Mr. Razak did not talk to any security officers at the Santa Ana Train Depot that day. The SAR notes the make and model of Mr. Razak's vehicle, and his license plate number. On information and belief, Security Officer De La Rosa followed Mr. Razak to his vehicle and wrote down his license plate number to identify him.

132. At no point while he was waiting in the Train Depot did Mr. Razak engage in conduct that gave rise to a reasonable suspicion of criminal activity.

133. This SAR falls into one or more of the behavioral categories identified in Functional Standard 1.5, in particular, "Observation/Surveillance." Functional Standard 1.5 at 30. It also falls under DOJ's "Potential Indicators of Terrorist Activities Related to Mass Transportation," which includes, among other things, "[u]nusual or prolonged interest in … [e]ntry points and access controls." It also falls under one or more behavioral categories

identified by Defendant DOJ, such as the catch-all behavioral category of "acting suspiciously." The SAR about Mr. Razak was collected, maintained, and disseminated through a fusion center SAR database, and on information and belief has been uploaded to eGuardian and/or another national SAR database.

134. Because Mr. Razak is the subject of a SAR that falls under Defendants' standards for suspicious activity reporting, Mr. Razak has been automatically subjected to law enforcement scrutiny. That scrutiny may include but is not limited to scrutiny or interviews by any of the law enforcement agencies across the country that have access to the SAR about him.

135. Mr. Razak is deeply troubled by what may result from the collection, maintenance, and dissemination in a national database of a report describing him as engaging in suspicious activity with a potential nexus to terrorism.

136. Upon information and belief, the SAR about Mr. Razak is maintained and will continue to be maintained in one or more national SAR databases, where it can be accessed by law enforcement agencies across the country.

5. Aaron Conklin

137. Aaron Conklin resides in Vallejo, California. Mr. Conklin is a student at Diablo Valley College, studying graphic design. He is also an amateur photographer who posts his work online. Mr. Conklin has a strong aesthetic interest in photographing industrial architecture, including refineries.

138. In either 2011 or 2012, Mr. Conklin was photographing the Valero Refinery located in Benicia, California at around 10:00 p.m. He chose to photograph at night for aesthetic reasons, to capture the refinery illuminated against the dark night sky. Mr. Conklin set up in an empty lot where a food truck parks during the day, near a publicly accessible sidewalk and a bus stop. Mr. Conklin was positioned outside the refinery's fenced perimeter.

139. Despite Mr. Conklin's location outside the refinery's perimeter in a publicly accessible location, a private security guard from the refinery came out to tell Mr. Conklin that he could not photograph the refinery and issued stern warnings. Mr. Conklin felt threatened and feared that the situation would escalate if he remained, so he left. Because he fears further

harassment, he has not returned to photograph the refinery, despite his desire to develop his portfolio with photographs of industrial sites.

140. Mr. Conklin later discovered that images of the refinery, taken from a similar location, were viewable on the internet through Google Maps, using the site's "street view" feature.

141. In or about November 2013, Mr. Conklin was attempting to photograph the Shell Refinery located in Martinez, California at approximately 9:30 or 10:00 pm. He wished to photograph the refinery at night for artistic reasons.

142. Mr. Conklin set up in the parking lot of a strip mall containing a smog testing center and a dance studio, across the street from the Shell Refinery's fenced perimeter.

143. As Mr. Conklin was preparing to photograph, a private security guard came out from the refinery and stopped him. At least one other guard from the refinery soon joined the first security guard. The security guards told Mr. Conklin that he was prohibited from photographing the refinery and that photographing the refinery was illegal and somehow connected to terrorism.

144. Despite Mr. Conklin's complete cooperation with the security guards, they called the Contra Costa County Sheriff's department, and at least two deputies arrived on the scene. The deputies searched through the pictures on Mr. Conklin's camera and searched his car. They also took pictures of Mr. Conklin, his camera equipment, and his vehicle. Mr. Conklin was afraid and felt as though he did not have the option to object to the searches without making matters worse for himself.

145. The deputies concluded by telling Mr. Conklin that he would have to be placed on an "NSA watch list." Only then was Mr. Conklin allowed to leave. The entire encounter lasted between forty-five minutes and an hour.

146. At no point while he was attempting to photograph the Valero or Shell refineries did Mr. Conklin engage in conduct that gave rise to a reasonable suspicion of criminal activity.

147. Taking photographs of infrastructure falls under one or more of the behavioral categories identified by Defendant PM-ISE as "suspicious," and also falls under one or more

behavioral categories identified by Defendant DOJ, such as the catch-all behavioral category of "acting suspiciously." A Contra Costa deputy sheriff expressly told Mr. Conklin that he had to be put on an "NSA watchlist." On information and belief, Mr. Conklin is the subject of a SAR, which was collected, maintained, and disseminated through a fusion center SAR database, and uploaded to eGuardian and/or another national SAR database.

148. On information and belief, security guards at oil refineries are trained in Defendants' standards for SAR reporting. As a result, security guards at the Valero and Shell oil refineries prevented Mr. Conklin from taking photographs of sites of aesthetic interest to him. On information and belief, the Contra Costa deputy sheriffs are trained in Defendants' standards for SAR reporting. As a result, they detained and searched Mr. Conklin for doing nothing more than attempting to photograph a site of aesthetic interest from a public location, told Mr. Conklin that he had to be placed on a watchlist, and reported Mr. Conklin in a SAR.

149. Because Mr. Conklin is the subject of a SAR that falls under Defendants' standards for suspicious activity reporting, Mr. Conklin has been automatically subjected to law enforcement scrutiny. That scrutiny may include but is not limited to scrutiny or interviews by any of the law enforcement agencies across the country that have access to the SAR about him.

150. Mr. Conklin was very upset by the encounter with private security and Contra Costa deputy sheriffs at the Shell refinery. He wants to continue taking photographs of industrial architecture in the future. But because of this event and the earlier incident at the Valero refinery, he is afraid to continue photographing industrial sites for fear of being stopped and questioned or, worse, arrested. Mr. Conklin has been chilled and has refrained from engaging in certain forms of photography, despite his desire to develop his photography portfolio. His inability to develop his photography portfolio limits his ability to apply successfully for jobs in his chosen field.

151. Mr. Conklin is also deeply troubled by what may result from the collection, maintenance, and dissemination in a national database of a report describing him as engaging in suspicious activity with a potential nexus to terrorism.

152. Mr. Conklin currently worries about being on a watchlist because he fears it will adversely impact him in the future. For example, he is concerned about his employment prospects if employers conduct background checks and he is flagged as someone with a potential connection to terrorism. Mr. Conklin also currently worries about being on a watchlist because he fears it will adversely impact his family. His father has worked and is seeking employment in the aviation industry and as a result must undergo rigorous background checks; Mr. Conklin is afraid about jeopardizing his father's career based on his own innocent efforts to take photographs of aesthetically interesting sites.

FIRST CLAIM FOR RELIEF

Violation of APA by Defendants DOJ and Eric Holder for Agency Action that is Arbitrary and Capricious and Not in Accordance with Law 5 U.S.C. §§ 702, 706(2)(A)

153. Plaintiffs incorporate by reference all preceding paragraphs as if fully set forth herein.

154. DOJ's promulgation of DOJ's SAR Standard constitutes final agency action.

155. DOJ and Eric Holder have issued a SAR Standard that sets forth operating principles for the collection, maintenance, and dissemination of "criminal intelligence information" within the meaning of 28 CFR Part 23. It applies to entities that operate arrangements, equipment, facilities, and procedures used for the receipt, storage, interagency exchange or dissemination and analysis of criminal intelligence information. These entities and the systems they operate receive support from OJP and constitute "projects" and "criminal intelligence systems" within the meaning of 28 CFR Part 23.

156. Because DOJ's SAR standard is broader than 28 CFR Part 23 and authorizes the collection, maintenance, and dissemination of information even in the absence of reasonable suspicion of criminal activity, it conflicts with 28 CFR Part 23. DOJ has also undermined 28 CFR Part 23 by training participants in the NSI on DOJ's SAR Standard.

157. Defendants DOJ and Eric Holder have not provided a reasoned basis for adopting a conflicting standard.

158. Defendants' actions described herein were and are arbitrary, capricious, an

abuse of discretion, and otherwise not in accordance with law, and should be set aside as unlawful pursuant to 5 U.S.C. § 706 (2012).

SECOND CLAIM FOR RELIEF

Violation of APA by Defendants PM-ISE and Kshemendra Paul for Agency Action that is Arbitrary and Capricious and Not in Accordance with Law 5 U.S.C. §§ 702, 706(2)(A)

159. Plaintiffs incorporate by reference all preceding paragraphs as if fully set forth herein.

160. PM-ISE's promulgation of Functional Standard 1.5 constitutes final agency action.

161. PM-ISE and Kshemendra Paul have issued a SAR Standard that sets forth operating principles for the collection, maintenance, and dissemination of "criminal intelligence information" within the meaning of 28 CFR Part 23. It applies to entities that operate arrangements, equipment, facilities, and procedures used for the receipt, storage, interagency exchange or dissemination and analysis of criminal intelligence information. These entities and the systems they operate receive support from OJP and constitute "projects" and "criminal intelligence systems" within the meaning of 28 CFR Part 23.

162. Because Functional Standard 1.5 is broader than 28 CFR Part 23 and authorizes the collection, maintenance, and dissemination of information even in the absence of reasonable suspicion of criminal activity, it conflicts with 28 CFR Part 23. PM-ISE has also undermined 28 CFR Part 23 by training participants in the NSI on Functional Standard 1.5.

163. Defendants PM-ISE and Kshemendra Paul have not provided a reasoned basis for adopting a conflicting standard.

164. Defendants' actions described herein were and are arbitrary, capricious, an abuse of discretion, otherwise not in accordance with law and should be set aside as unlawful pursuant to 5 U.S.C. § 706 (2012).

//

//

//

THIRD CLAIM FOR RELIEF

Violation of APA by Defendants DOJ and Eric Holder
for Issuance of a Legislative Rule Without Notice and Comment
5 U.S.C. §§ 553, 706(2)(A), (D)

165. Plaintiffs incorporate by reference all preceding paragraphs as if fully set forth herein.

166. DOJ's SAR's Standard is a legislative rule but was adopted without observing the notice and comment procedure required under 5 U.S.C. § 553 (2012). Because DOJ's SAR Standard was adopted without observing the required notice and comment procedure, Defendants' actions described herein were and are also arbitrary, capricious, an abuse of discretion, otherwise not in accordance with law, and without observance of procedure required by law. Defendants' actions should be set aside as unlawful pursuant to 5 U.S.C. § 706 (2012).

FOURTH CLAIM FOR RELIEF

Violation of APA by Defendants PM-ISE and Kshemendra Paul
for Issuance of a Legislative Rule Without Notice and Comment
5 U.S.C. §§ 553, 706(2)(A), (D)

167. Plaintiffs incorporate by reference all preceding paragraphs as if fully set forth herein.

168. PM-ISE's Functional Standard 1.5 is a legislative rule but was adopted without observing the notice and comment procedure required under 5 U.S.C. § 553 (2012). Because PM-ISE's Functional Standard 1.5 was adopted without observing the required notice and comment procedure, Defendants' actions described herein were and are also arbitrary, capricious, an abuse of discretion, otherwise not in accordance with law, and without observance of procedure required by law. Defendants' actions should be set aside as unlawful pursuant to 5 U.S.C. § 706 (2012).

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs pray that the Court:

1. Enter a declaratory judgment that DOJ's standard for SAR reporting is invalid and issue a permanent injunction requiring Defendants DOJ and Eric Holder to rescind DOJ's SAR Standard and cease and desist from training participants in the NSI in DOJ's SAR Standard.

2. Enter a declaratory judgment that Functional Standard 1.5 is invalid and issue a permanent injunction requiring Defendants PM-ISE and KSHEMENDRA PAUL to rescind Functional Standard 1.5 and cease and desist from training participants in the NSI in Functional Standard 1.5.

3. Enter a declaratory judgment that 28 CFR Part 23 sets forth the standard for SAR reporting.

4. Enter a permanent injunction requiring Defendants to use 28 CFR Part 23 as the standard for SAR reporting.

5. Award Plaintiffs their costs and expenses, including reasonable attorneys' fees and expert witness fees; and

6. Award such further and additional relief as is just and proper.

Respectfully submitted,

DATED: July 10, 2014

BINGHAM MCCUTCHEN LLP
Jonathan Loeb (SBN 162758)
jon.loeb@bingham.com
Jeffrey Rosenfeld (SBN 221625)
jeffrey.rosenfeld@bingham.com
Edward Andrews (SBN 268479)
edward.andrews@bingham.com
The Water Garden
Suite 2050 North
1601 Cloverfield Boulevard
Santa Monica, CA 90404-4082
Telephone: 310-907-1000
Facsimile: 310-907-2000

BINGHAM MCCUTCHEN LLP
Stephen Scotch-Marmo (*pro hac vice pending*)
stephen.scotch-marmo@bingham.com
Michael James Ableson (*pro hac vice pending*)
michael.ableson@bingham.com
399 Park Avenue
New York, NY 10022-4689
Telephone: 212-705-7000
Facsimile: 212-752-5378

AMERICAN CIVIL LIBERTIES UNION
FOUNDATION OF NORTHERN CALIFORNIA
Linda Lye (SBN 215584)
llye@aclunc.org
Julia Harumi Mass (SBN 189649)
jmass@aclunc.org
39 Drumm Street
San Francisco, CA 94111
Telephone: 415-621-2493
Facsimile: 415-255-8437

ASIAN AMERICANS ADVANCING
JUSTICE - ASIAN LAW CAUCUS
Nasrina Bargzie (SBN 238917)
nasrinab@advancingjustice-alc.org
Yaman Salahi (SBN 288752)
yamans@advancingjustice-alc.org
55 Columbus Avenue
San Francisco, CA 94111
Telephone: 415-848-7711
Facsimile: 415-896-1702

AMERICAN CIVIL LIBERTIES UNION
FOUNDATION
Hina Shamsi (*pro hac vice pending*)
hshamsi@aclu.org
Hugh Handeyside (*pro hac vice pending*)
hhandeyside@aclu.org
125 Broad Street
New York, NY 10004
Telephone: 212-549-2500
Facsimile: 212-549-2654

AMERICAN CIVIL LIBERTIES UNION
FOUNDATION OF SAN DIEGO AND IMPERIAL
COUNTIES
Mitra Ebadolahi (SBN 275157)
mebadolahi@aclusandiego.org
P.O. Box 87131
San Diego, CA 92138
Telephone: (619) 232-2121
Facsimile: (619) 232-0036

AMERICAN CIVIL LIBERTIES UNION
FOUNDATION OF SOUTHERN CALIFORNIA
Peter Bibring (SBN 223981)
pbibring@aclusocal.org
1313 West 8th Street
Los Angeles, CA 90017
Telephone: (213) 977-9500
Facsimile: (213) 977-5299

By:___________*/s/ Jonathan Loeb*__________

Jonathan Loeb

BINGHAM MCCUTCHEN LLP

By:___________*/s/ Linda Lye*______________

Linda Lye

AMERICAN CIVIL LIBERTIES UNION
FOUNDATION OF NORTHERN CALIFORNIA

By:___________*/s/ Nasrina Bargzie*__________

Nasrina Bargzie

ASIAN AMERICANS ADVANCING JUSTICE –
ASIAN LAW CAUCUS

Attorneys for Plaintiffs Wiley Gill, James Prigoff, Tariq Razak, Khaled Ibrahim, and Aaron Conklin

DECLARATION PURSUANT TO LOCAL RULE 5-1(i)(3)

Pursuant to Local Rule 5-1(i)(3), the undersigned filer declares that concurrence in the filing of this document has been obtained from the other signatories to this document.

I declare under penalty of perjury under the laws of the United States that the foregoing is true and correct. Executed this 10th day of July 2013.

__________*/s/ Jonathan Loeb*______

Jonathan Loeb

Exhibit A

Central California Intelligence Center

www.sacrtac.org ◆ (916) 808-8383 or (888) 884-8383 ◆ Fax (916) 874-6180

January 3, 2014

Mr. Yaman Salahi
Staff Attorney
Asian Americans Advancing Justice
Asian Law Caucus
55 Columbus Ave.
San Francisco, CA 94111
(415) 896-1701

Dear Mr. Salahi:

This letter is in response to the Public Records Act request received from the Asian Law Caucus dated December 3, 2013.

After reviewing your Public Records Act request it appears the request is for additional SAR data, from the timeframes of June 2010 to June 2012, stored in the CCIC databases and previously submitted to the ACLU in August 2012. You have specifically requested the following:

"This letter constitutes a request under the California Public Records Act, Cal. Gov. Code 6250, et seq., and Article I s 3(b) of the California Constitution on behalf of Mr. Wiley Wayne Gill for all records, including but not limited to Suspicious Activity Reports, pertaining to or referencing Mr. Gill."

The CCIC/RTAC has located only one (1) Suspicious Activity Report (SAR) related to Mr. Gill. Please see the attached redacted SAR (enclosure 1). After a thorough review of our records, there is no further information available regarding Mr. Wiley Wayne Gill.

Respectfully,

/Herbert M Brown HH

Herb Brown, Executive Director
Central California Intelligence Center
(916) 874-1287

Enclosures (1)

ENCLOSURE 1

Memex Record	Date Created	Activity Date	Title	Disposition	eGuardian	Activity
CCSA0000 2180	5/23/2012	5/20/2012	Suspicious Male Subject in Possession of Flight Simulator Game	pending		During early 2011 I made a professional visit to the [redacted] at [redacted] (I was in a full patrol uniform). During the visit I found the members to be welcoming and appreciative of the visit with the esception of one subject later identified as [redacted]; CDL # [redacted]. [redacted] was hesitant to interact with law enforcement, avoided eye contact, and appeared to be eavesdropping while I spoke with other members. I beleive [redacted] reported he was a previous student of [redacted]. [redacted] is a [redacted] who based on his appearence (full beard and traditional garb) is a full convert to Islam at the young age of 26. [redacted] dis not have a job at the time and was living on site at [redacted]. Since this itneraction I have seen [redacted] several times walking through [redacted] in traditional garb walking with elders of [redacted]. I approached the group on at least one occasion and found [redacted] to avoid eye contact and hesitant to answer questions. On 5/20/12 [redacted] was investigating a domestic violence incident that took him to [redacted] in search of a suspect. During the search he conducted a cursory search of [redacted]'s house as there was some indicationt he suspect may have fled into the residence (later determined to be unfounded). [redacted] found the house immaculate. [redacted] was not very happy with [redacted] entering the house, presumably becuase he still ahd his shoes on. [redacted] noticed [redacted] had a computer console located in the residence. As [redacted] attempted to hastly close down the screen [redacted] noted [redacted] was on a [redacted] page titled somehting similar to "Games that fly under the radar." [redacted] noted [redacted] appeared to be accessing a flight simulator type of game. [redacted] full conversion to Islam as a young WMA and pious demeanor is rare. Coupled with the fact he is unemployed, appears to shun law enforcement contact, has potential access to flight simulators via the internet which he tried to minimize is worthy of note.

Exhibit B

Central California Intelligence Center
www.sacrtac.org ♦ (916) 808-8383 or (888) 884-8383 ♦ Fax (916) 874-6180

February 25, 2014

Mr. Yaman Salahi
Staff Attorney
Asian Americans Advancing Justice
Asian Law Caucus
55 Columbus Ave.
San Francisco, CA 94111
(415) 896-1701

Dear Mr. Salahi:

This letter is in response to the Public Records Act request received from the Asian Law Caucus dated January 22, 2014.

After reviewing your Public Records Act request it appears you have specifically requested the following:

"This letter constitutes a request under the California Public Records Act, Cal. Gov. Code 6250, et seq., and Article I s 3(b) of the California Constitution on behalf of Mr. Khaled Ibrahim for all records, including but not limited to Suspicious Activity Reports, pertaining to or referencing Mr. Ibrahim."

The CCIC/RTAC has located only one (1) Suspicious Activity Report (SAR) related to Mr. Ibrahim. Please see the attached redacted SAR (enclosure 1). After a thorough review of our records, there is no further information available regarding Mr. Khaled Ibrahim.

Respectfully,

Herb Brown, Executive Director
Central California Intelligence Center
(916) 874-1287

Enclosures (1)

ENCLOSURE 1

Memex Record Number	Date Created	Activity Date	Title	Disposition	Activity
CCSA00001881	11/14/2011	11/6/2011	Suspicious attempt to purchase large number of computers	eGuardian Entry	Contact was made with [redacted] by [redacted] during the week of 11-6-11 through 11-12-11 at the same [redacted] located in [redacted] [redacted] Ca. [redacted] wanted to buy a large amount of computers from [redacted]. [redacted] told him to leave and did not sell any computers to [redacted] This is the [redacted] has made with [redacted] The second contact with [redacted] [redacted] occured in [redacted]. Thank you for your time. I have since [redacted] and work as a [redacted] Information submitted to [redacted] on [redacted] For [redacted] Located [redacted] Ca. I received a follow up from the [redacted] Located in [redacted] regarding the incident. I am a [redacted] located at [redacted] located at [redacted] located in [redacted]. I have a friend whose name is named [redacted] and works as a [redacted] at [redacted] Located at [redacted] [redacted], [redacted] A customer [redacted] looking to buy merchandice [redacted] to be shipped to [redacted] [redacted] old me that [redacted] bought over [redacted] to be [redacted] [redacted] at that time. [redacted] said it would be OK for you to contact him for additional information [redacted] from [redacted] [redacted] said he cannot provide certain info because of customer privacy laws. Here is some additional information listed below: [redacted] said that the guy's name is [redacted] of [redacted] The [redacted] provided [redacted] is: [redacted] 's [redacted] s [redacted] is [redacted] [redacted] won't divulge [redacted] that the purchased all of the computers are shipped to the [redacted] When [redacted] asked [redacted] why he doesn't [redacted] [redacted] [redacted] or [redacted] responded and said that those companies [redacted] and because the

					[redacted] they can't sell to him directly. [redacted] requests [redacted] [redacted] continues to contact him to see if [redacted] has [redacted] Please feel free to contact me at [redacted] Thank you for your time. [redacted]

Exhibit C

Santa Ana Police Department
60 Civic Center Plaza -- Santa Ana, CA 92701

Case No. 2011-15770

Information Report

Case Type: Suspicious Activity Report
Prepared by: Ofc. J. Gallardo #3203
Section: Patrol Watch 1/NE
Date prepared: 5/16/2011 1502 hours

Reviewed by: R. Rodriguez 2755 Date/Time: 5-16-11 1720 (Rev. 0.60)

Records Distribution: Review: 1782 Total Copies: 2 By: 1882 Date: ______

☐ Animal Control	☐ Court Liaison	☐ Orangewood	☐ Traffic	☐ Trackers
☑ District Inv.	☐ CAP	☐ Evidence	☐ Vice	☐ Sex Crimes
☐ Domestic Violence	☐ Crime Prevention	☐ Narcotics	☐ Juvenile Inv.	☐ Graffiti
☐ Career Criminal Unit	☐ Crime Analysis	☐ Gangs	☐ Fax/Name ______	
☐ Juvenile Hall	☐ Stats	☐ Rap	☑ Other Homeland Sec	
#310000000000024029	☐ Other ______		☐ Other ______	

Incident Activity Summary:

Special Attention:

Information Report: Train Station Subject

Incident Date/Time: Occurred: 05/16/2011 10:20 to 05/16/2011 10:30
Reported: 05/16/2011 12:18

Location Occurred: 1000 E. Santa Ana Boulevard, Santa Ana, CA 92702-0000
Grid: 205 Dist.: 2

Factual Synopsis: Male of Middle Eastern decent observed surveying entry/exit points.

Person: **Karina De La Rosa**
Involvement: **Contact**
Person Note: *Security Officer*
Gender/Race: Female / Hispanic
DOBs:
Address:
Grid: 205 Dist.: 2
Contact Info:

Description: Physical: 5'05" tall, 125 lbs., thin build, long brown straight hair, black eyes,

Person: **Tariq Razak**
Involvement: **Mentioned**
Person Note:

	Close Cropped Beard.
Gender/Race:	Male / Arab
Address:	Location association: Resides
Description:	[redacted] Physical: 5'11" tall, 175 lbs., medium build, short black straight hair, brown eyes, beard,

---

Person:	**Unknown**
Involvement:	**Mentioned**
Person Note:	*Uknown information about female.*
Gender/Race:	Female / Arab

Vehicle:	**Passenger Car**
Involvement:	**Involved** / Retained by Owner
Description:	2007 Honda Accord, 4 Door Sedan or Hatchback, White/White
License Plate:	CA, Reg 07/2011
Registered owner:	
Legal owner:	

Narrative:

On 5-16-11 at about 1220 hours, I responded to The Santa Ana Train Depot at 1000 E Santa Ana Blvd.

I contacted Security Officer Karina De La Rosa who told me the following:

At approximately 1020 hours, Karina took the elevator from the second floor to the first floor. In the elevator with Karina was a male between male of who Karina believed was of Middle Eastern descent. Karina's suspicion became aroused because the male appeared to be observant of his surroundings and was constantly surveying all areas of the facility. The male's appearance was neat and clean with a closely cropped beard, short hair wearing blue jeans and a blue plaid shirt.

Upon exiting the elevator, Karina observed the male meticulously study the entry/exit points, different lobby areas of the train station where large groups of passengers gather. The male then went to the north end of station where male and female restrooms are located and stood by outside the restrooms. Minutes later, a female wearing a white burka head dress, black pants and a blue shirt exited the restroom.

The two individuals then both exited the train station out of the north doors, entered a white 2007 Honda Accord (Ca Li) and left the Train Station in an unknown direction.

Karina continued to say that she received 'suspicious activity as related to terrorism training' by a local police agency. Karina said the behavior depicted by the male was similar to examples shown in her training raising her suspicion and making the decision to notify police. Attached to this report is a photocopy of Karina's incident report.

Request this report be forwarded to SAPD Homeland Security Division and to the Orange County Intelligence Assessment Center (OCIAC) for review and possible follow-up.

Ofcr. J. Gallardo # 3203
Terrorism Liaison Officer (TLO)
Santa Ana Police Department

Exhibit D

INFORMATION SHARING ENVIRONMENT (ISE)

FUNCTIONAL STANDARD (FS)

SUSPICIOUS ACTIVITY REPORTING (SAR)

VERSION 1.5

1. Authority. Homeland Security Act of 2002, as amended; The Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA), as amended; Presidential Memorandum dated April 10, 2007 (Assignment of Functions Relating to the Information Sharing Environment); Presidential Memorandum dated December 16, 2005 (Guidelines and Requirements in Support of the Information Sharing Environment); DNI memorandum dated May 2, 2007 (Program Manager's Responsibilities); Executive Order 13388; and other applicable provisions of law, regulation, or policy.

2. Purpose. This issuance serves as the updated Functional Standard for ISE-SARs, and one of a series of Common Terrorism Information Sharing Standards (CTISS) issued by the PM-ISE. While limited to describing the ISE-SAR process and associated information exchanges, information from this process may support other ISE processes to include alerts, warnings, and notifications, situational awareness reporting, and terrorist watchlisting.

3. Applicability. This ISE-FS applies to all departments or agencies that possess or use terrorism or homeland security information, operate systems that support or interface with the ISE, or otherwise participate (or expect to participate) in the ISE, as specified in Section 1016(i) of the IRTPA.

4. References. ISE Implementation Plan, November 2006; ISE Enterprise Architecture Framework (EAF), Version 2.0, September 2008; Initial Privacy and Civil Liberties Analysis for the Information Sharing Environment, Version 1.0, September 2008; ISE-AM-300: Common Terrorism Information Standards Program, October 31, 2007; Common Terrorism Information Sharing Standards Program Manual, Version 1.0, October 2007; National Information Exchange Model, Concept of Operations, Version 0.5, January 9, 2007; 28 Code of Federal Regulations (CFR) Part 23; Executive Order 13292 (Further Amendment to Executive Order 12958, as Amended, Classified National Security Information); Nationwide Suspicious Activity Reporting Concept of Operations, December 2008; ISE Suspicious Activity Reporting Evaluation Environment (EE) Segment Architecture, December 2008.

5. Definitions.

a. Artifact: Detailed mission product documentation addressing information exchanges and data elements for ISE-SAR (data models, schemas, structures, etc.).

b. CTISS: Business process-driven, performance-based "common standards" for preparing terrorism information for maximum distribution and access, to enable the acquisition, access, retention, production, use, management, and sharing of terrorism information within the ISE. CTISS, such as this *ISE-SAR Functional Standard*, are implemented in ISE participant infrastructures that include ISE Shared Spaces as described in the *ISE EAF*. Two categories of common standards are formally identified under CTISS:

   (1) Functional Standards – set forth rules, conditions, guidelines, and characteristics of data and mission products supporting ISE business process areas.

   (2) Technical Standards – document specific technical methodologies and practices to design and implement information sharing capability into ISE systems.

c. Information Exchange: The transfer of information from one organization to another organization, in accordance with CTISS defined processes.

d. ISE-Suspicious Activity Report (ISE-SAR): An ISE-SAR is a SAR (as defined below in 5i) that has been determined, pursuant to a two-part process, to have a potential terrorism nexus (i.e., to be reasonably indicative of criminal activity associated with terrorism). ISE-SAR business, privacy, and civil liberties rules will serve as a unified process to support the reporting, tracking, processing, storage, and retrieval of terrorism-related suspicious activity reports across the ISE.

e. National Information Exchange Model (NIEM): A joint technical and functional standards program initiated by the Department of Homeland Security (DHS) and the Department of Justice (DOJ) that supports national-level interoperable information sharing.

f. Personal Information: Information that may be used to identify an individual (i.e., data elements in the identified "privacy fields" of this *ISE-SAR Functional Standard*).

g. Privacy Field: A data element that may be used to identify an individual and, therefore, may be subject to privacy protection.

h. Suspicious Activity: Observed behavior reasonably indicative of pre-operational planning related to terrorism or other criminal activity.

i. Suspicious Activity Report (SAR): Official documentation of observed behavior reasonably indicative of pre-operational planning related to terrorism or other criminal activity.

j. Universal Core (UCore): An interagency information exchange specification and implementation profile. It provides a framework for sharing the most commonly used data concepts of "who, what when, and where". UCore serves as a starting point for data level integration and permits the development of richer domain specific exchanges. UCore was developed in concert with NIEM program office, and is a collaborative effort between Department of Defense (DOD), DOJ, DHS and the Intelligence Community.

6. Guidance. This Functional Standard is hereby established as the nationwide ISE Functional Standard for ISE-SARs. It is based on documented information exchanges and business requirements, and describes the structure, content, and products associated with processing, integrating, and retrieving ISE-SARs by ISE participants.

7. Responsibilities.

a. The PM-ISE, in consultation with the Information Sharing Council (ISC), will:

(1) Maintain and administer this *ISE-SAR Functional Standard*, to include:

(a) Updating the business process and information flows for ISE-SAR.

(b) Updating data elements and product definitions for ISE-SAR.

(2) Publish and maintain configuration management of this *ISE-SAR Functional Standard*.

(3) Assist with the development of ISE-SAR implementation guidance and governance structure, as appropriate, to address privacy, civil rights, and civil liberties, policy, architecture, and legal issues.

(4) Work with ISE participants, through the CTISS Committee, to develop a new or modified *ISE-SAR Functional Standard*, as needed.

(5) Coordinate, publish, and monitor implementation and use of this *ISE-SAR Functional Standard*, and coordinate with the White House Office of Science and Technology Policy and with the National Institute of Standards and Technology (in the Department of Commerce) for broader publication, as appropriate.

b. Each ISC member and other affected organizations shall:

(1) Propose modifications to the PM-ISE for this Functional Standard, as appropriate.

(2) As appropriate, incorporate this *ISE-SAR Functional Standard*, and any subsequent implementation guidance, into budget activities associated with relevant current (operational) mission specific programs, systems, or initiatives (e.g. operations and maintenance {O&M} or enhancements).

(3) As appropriate, incorporate this *ISE-SAR Functional Standard*, and any subsequent implementation guidance, into budget activities associated with future or new development efforts for relevant mission specific programs, systems, or initiatives (e.g. development, modernization, or enhancement {DME}).

(4) Ensure incorporation of this *ISE-SAR Functional Standard*, as set forth in 7.b (2) or 7.b (3) above, is done in compliance with ISE Privacy Guidelines and any additional guidance provided by the ISE Privacy Guidelines Committee.

8. Effective Date and Expiration. This ISE-FS is effective immediately and will remain in effect as the updated *ISE-SAR Functional Standard* until further updated, superseded, or cancelled.

Program Manager for the
Information Sharing Environment

Date: May 21, 2009

PART A – ISE-SAR FUNCTIONAL STANDARD ELEMENTS

SECTION I – DOCUMENT OVERVIEW

A. List of ISE-SAR Functional Standard Technical Artifacts

The full ISE-SAR information exchange contains five types of supporting technical artifacts. This documentation provides details of implementation processes and other relevant reference materials. A synopsis of the *ISE-SAR Functional Standard* technical artifacts is contained in Table 1 below.

Table 1 – Functional Standard Technical Artifacts[1]

Artifact Type	Artifact	Artifact Description
Development and Implementation Tools	1. Component Mapping Template (CMT) (SAR-to-NIEM/UCore)	This spreadsheet captures the ISE-SAR information exchange class and data element (source) definitions and relates each data element to corresponding National Information Exchange Model (NIEM) Extensible Mark-Up Language (XML) elements and UCore elements, as appropriate.
	2. NIEM Wantlist	The Wantlist is an XML file that lists the elements selected from the NIEM data model for inclusion in the Schema Subset. The Schema Subset is a compliant version to both programs that has been reduced to only those elements actually used in the ISE-SAR document schema.
	3. XML Schemas	The XML Schema provides a technical representation of the business data requirements. They are a machine readable definition of the structure of an ISE-SAR-based XML Message.
	4. XML Sample Instance	The XML Sample Instance is a sample document that has been formatted to comply with the structures defined in the XML Schema. It provides the developer with an example of how the ISE-SAR schema is intended to be used.
	5. Codified Data Field Values	Listings, descriptions, and sources as prescribed by data fields in the *ISE-SAR Functional Standard*.

1 Development and implementation tools may be accessible through www.ise.gov. Additionally, updated versions of this Functional Standard will incorporate the CTISS Universal Core which harmonizes the NIEM Universal Core with the DoD/IC UCore.

SECTION II – SUSPICIOUS ACTIVITY REPORTING EXCHANGES

A. ISE-SAR Purpose

This *ISE-SAR Functional Standard* is designed to support the sharing, throughout the Information Sharing Environment (ISE), of information about suspicious activity, incidents, or behavior (hereafter collectively referred to as suspicious activity or activities) that have a potential terrorism nexus. The ISE includes State and major urban area fusion centers and their law enforcement,[2] homeland security,[3] or other information sharing partners at the Federal, State, local, and tribal levels to the full extent permitted by law. In addition to providing specific indications about possible terrorism-related crimes, ISE-SARs can be used to look for patterns and trends by analyzing information at a broader level than would typically be recognized within a single jurisdiction, State, or territory. Standardized and consistent sharing of suspicious activity information regarding criminal activity among State and major urban area fusion centers and Federal agencies is vital to assessing, deterring, preventing, or prosecuting those involved in criminal activities associated with terrorism. This *ISE-SAR Functional Standard* has been designed to incorporate key elements that describe potential criminal activity associated with terrorism and may be used by other communities to address other types of criminal activities where appropriate.

B. ISE-SAR Scope

Suspicious activity is defined as *observed behavior reasonably indicative of pre-operational planning related to terrorism or other criminal activity*. A determination that such suspicious activity constitutes an ISE-SAR is made as part of a two-part process by trained analysts using explicit criteria. Some examples of the criteria for identifying those SARs, with defined relationships to criminal activity that also have a potential terrorism nexus, are listed below. Part B (ISE-SAR Criteria Guidance) provides a more thorough explanation of ISE-SAR criteria, highlighting the importance of context in interpreting such behaviors;

- Expressed or implied threat
- Theft/loss/diversion
- Site breach or physical intrusion
- Cyber attacks
- Probing of security response

---

[2] All references to Federal, State, local and tribal law enforcement are intended to encompass civilian law enforcement, military police, and other security professionals.

[3] All references to homeland security are intended to encompass public safety, emergency management, and other officials who routinely participate in the State or major urban area's homeland security preparedness activities.

It is important to stress that this *behavior-focused approach* to identifying suspicious activity requires that factors such as race, ethnicity, national origin, or religious affiliation should not be considered as factors that create suspicion (except if used as part of a specific suspect description). It is also important to recognize that many terrorism activities are now being funded via local or regional criminal organizations whose direct association with terrorism may be tenuous. This places law enforcement and homeland security professionals in the unique, yet demanding, position of identifying suspicious activities or materials as a byproduct or secondary element in a criminal enforcement or investigation activity. This means that, while some ISE-SARs may document activities or incidents to which local agencies have already responded, there is value in sharing them more broadly to facilitate aggregate trending or analysis.

Suspicious Activity Reports are not intended to be used to track or record ongoing enforcement, intelligence, or investigatory operations although they can provide information to these activities. The ISE-SAR effort offers a standardized means for sharing information regarding behavior potentially related to terrorism-related criminal activity and applying data analysis tools to the information. Any patterns identified during ISE-SAR data analysis may be investigated in cooperation with the reporting agency, Joint Terrorism Task Force (JTTF), or the State or major urban area fusion center in accordance with departmental policies and procedures. Moreover, the same constitutional standards that apply when conducting ordinary criminal investigations also apply to local law enforcement and homeland security officers conducting SAR inquiries. This means, for example, that constitutional protections and agency policies and procedures that apply to a law enforcement officer's authority to stop, stop and frisk ("Terry Stop")[4], request identification, or detain and question an individual would apply in the same measure whether or not the observed behavior related to terrorism or any other criminal activity.

C. Overview of Nationwide SAR Cycle

As defined in the *Nationwide Suspicious Activity Reporting Initiative (NSI) Concept of Operations (CONOPS[5])* and shown in Figure 1, the nationwide SAR process involves a total of 12 discrete steps that are grouped under five standardized business process activities – Planning, Gathering and Processing, Analysis and Production, Dissemination, and Reevaluation. The top-level ISE-SAR business process described in this section has been revised to be consistent with the description in the *NSI CONOPS*. Consequently, the numbered steps in Figure 1 are the only ones that map directly to the nine-steps of the detailed information flow for nationwide SAR information sharing documented in Part C of this version of the *ISE-SAR Functional Standard*. For further detail on the 12 NSI steps, please refer to the *NSI CONOPS*.

---

4 "Terry Stop" refers to law enforcement circumstances related to Supreme Court of the United States ruling on "Terry v. Ohio (No. 67)" argued on December 12, 1967 and decided on June 10, 1968. This case allows a law enforcement officer to articulate reasonable suspicion as a result of a totality of circumstances (to include training and experience) and take action to frisk an individual for weapons that may endanger the officer. The Opinion of the Supreme Court regarding this case may be found at Internet site http://www.law.cornell.edu/supct/html/historics/USSC_CR_0392_0001_ZO.html.

5 PM-ISE, *Nationwide SAR Initiative Concept of Operations* (Washington: PM-ISE, 2008), available from www.ise.gov.

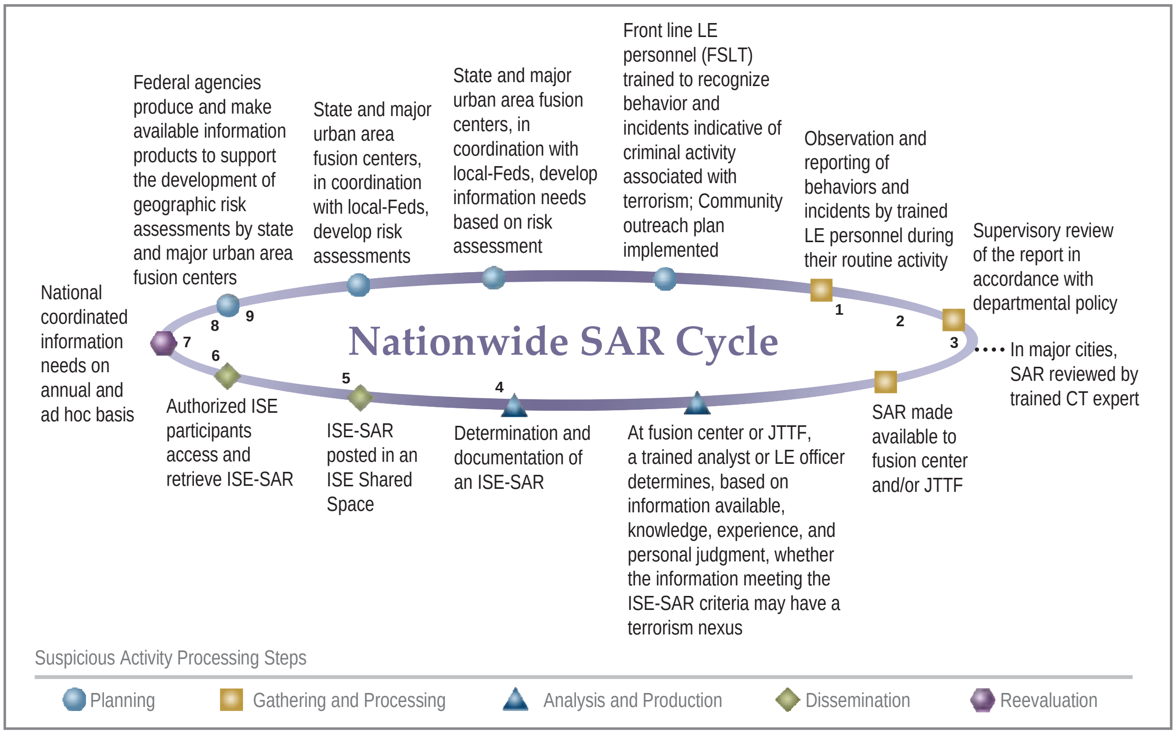

Federal agencies produce and make available information products to support the development of geographic risk assessments by state and major urban area fusion centers
State and major urban area fusion centers, in coordination with local-Feds, develop risk assessments
State and major urban area fusion centers, in coordination with local-Feds, develop information needs based on risk assessment
Front line LE personnel (FSLT) trained to recognize behavior and incidents indicative of criminal activity associated with terrorism; Community outreach plan implemented
Observation and reporting of behaviors and incidents by trained LE personnel during their routine activity
Supervisory review of the report in accordance with departmental policy
National coordinated information needs on annual and ad hoc basis
Nationwide SAR Cycle
1
2
3
4
5
6
7
8
9
In major cities, SAR reviewed by trained CT expert
Authorized ISE participants access and retrieve ISE-SAR
ISE-SAR posted in an ISE Shared Space
Determination and documentation of an ISE-SAR
At fusion center or JTTF, a trained analyst or LE officer determines, based on information available, knowledge, experience, and personal judgment, whether the information meeting the ISE-SAR criteria may have a terrorism nexus
SAR made available to fusion center and/or JTTF
Suspicious Activity Processing Steps
Planning
Gathering and Processing
Analysis and Production
Dissemination
Reevaluation

Figure 1. Overview of Nationwide SAR Process

D. ISE-SAR Top-Level Business Process

1. Planning

The activities in the planning phase of the NSI cycle, while integral to the overall NSI, are not discussed further in this Functional Standard. See the NSI CONOPS for more details.[6]

2. Gathering and Processing

Local law enforcement agencies or field elements of Federal agencies gather and document suspicious activity information in support of their responsibilities to investigate potential criminal activity, protect citizens, apprehend and prosecute criminals, and prevent crime. Information acquisition begins with an observation or report of unusual or suspicious behavior that may be indicative of criminal activity associated with terrorism. Such activities include, but are not limited to, theft, loss, or diversion, site breach or physical intrusion, cyber attacks, possible testing of physical response, or other unusual behavior or sector specific incidents. It is important to emphasize that context is an essential element of interpreting the relevance of such behaviors to criminal activity associated with terrorism. (See Part B for more details.)

[6] Ibid., 17-18.

Regardless of whether the initial observer is a private citizen, a representative of a private sector partner, a government official, or a law enforcement officer, suspicious activity is eventually reported to either a local law enforcement agency or a local, regional, or national office of a Federal agency. When the initial investigation or fact gathering is completed, the investigating official documents the event in accordance with agency policy, local ordinances, and State and Federal laws and regulations.

The information is reviewed within a local or Federal agency by appropriately designated officials for linkages to other suspicious or criminal activity in accordance with departmental policy and procedures.[7] Although there is always some level of local review, the degree varies from agency to agency. Smaller agencies may forward most SARs directly to the State or major urban area fusion center or JTTF with minimal local processing. Major cities, on the other hand, may have trained counterterrorism experts on staff that apply a more rigorous analytic review of the initial reports and filter out those that can be determined not to have a potential terrorism nexus.

After appropriate local processing, agencies make SARs available to the relevant State or major urban area fusion center. Field components of Federal agencies forward their reports to the appropriate regional, district, or headquarters office employing processes that vary from agency to agency. Depending on the nature of the activity, the information could cross the threshold of "suspicious" and move immediately into law enforcement operations channels for follow-on action against the identified terrorist activity. In those cases where the local agency can determine that an activity has a direct connection to criminal activity associated with terrorism, it will provide the information directly to the responsible JTTF for use as the basis for an assessment or investigation of a terrorism-related crime as appropriate.

3. Analysis and Production

The fusion center or Federal agency enters the SAR into its local information system and then performs an additional analytic review to establish or discount a potential terrorism nexus. First, an analyst or law enforcement officer reviews the newly reported information against ISE-SAR criteria outlined in Part B of this *ISE-SAR Functional Standard*. Second, the Terrorist Screening Center (TSC) should be contacted to determine if there is valuable information in the Terrorist Screening Database. Third, he or she will review the input against all available knowledge and information for linkages to other suspicious or criminal activity.

Based on this review, the officer or analyst will apply his or her professional judgment to determine whether the information has a potential nexus to terrorism. If the officer or analyst cannot make this explicit determination, the report will not be accessible by the ISE, although

[7] If appropriate, the agency may consult with a Joint Terrorism Task Force, Field Intelligence Group, or fusion center.

it may be retained in local fusion center or Federal agency files in accordance with established retention policies and business rules.[8]

4. Dissemination

Once the determination of a potential terrorism nexus is made, the information becomes an ISE-SAR and is formatted in accordance with the ISE-SAR Information Exchange Package Document (IEPD) format described in Sections III and IV. This ISE-SAR is then stored in the fusion center, JTTF, or other Federal agency's ISE Shared Space[9] where it can be accessed by authorized law enforcement and homeland security personnel in the State or major urban area fusion center's area of responsibility as well as other ISE participants, including JTTFs. This allows the fusion center to be cognizant of all terrorist-related suspicious activity in its area of responsibility, consistent with the information flow description in Part C. Although the information in ISE Shared Spaces is accessible by other ISE participants, it remains under the control of the submitting organization, i.e., the fusion center or Federal agency that made the initial determination that the activity constituted an ISE-SAR.

By this stage of the process, all initially reported SARs have been through multiple levels of review by trained personnel and, to the maximum extent possible, those reports without a potential terrorism nexus have been filtered out. Those reports posted in ISE Shared Spaces, therefore, can be presumed by Federal, State, and local analytic personnel to be terrorism-related and information derived from them can be used along with other sources to support counterterrorism operations or develop counterterrorism analytic products. As in any analytic process, however, all information is subject to further review and validation, and analysts must coordinate with the submitting organization to ensure that the information is still valid and obtain any available relevant supplementary material before incorporating it into an analytic product.

Once ISE-SARs are accessible, they can be used to support a range of counterterrorism analytic and operational activities. This step involves the actions necessary to integrate ISE-SAR information into existing counterterrorism analytic and operational processes, including efforts to "connect the dots," identify information gaps, and develop formal analytic products. Depending on privacy policy and procedures established for the NSI as a whole or by agencies responsible for individual ISE Shared Spaces, requestors may only be able to view reports in the Summary ISE-SAR Information format, i.e., without privacy fields. In these cases, requestors should contact the submitting organization directly to discuss the particular report more fully and obtain access, where appropriate, to the information in the privacy fields.

[8] As was already noted in the discussion of processing by local agencies, where the fusion center or Federal agency can determine that an activity has a direct connection to a possible terrorism-related crime, it will provide the information directly to the responsible JTTF for use as the basis for an assessment or investigation.

[9] PM-ISE, *ISE Enterprise Architecture Framework, Version 2.0*, (Washington: PM-ISE, 2008), 61-63

5. Reevaluation[10]

Operational feedback on the status of ISE-SARs is an essential element of an effective NSI process with important implications for privacy and civil liberties. First of all, it is important to notify source organizations when information they provide is designated as an ISE-SAR by a submitting organization and made available for sharing—a form of positive feedback that lets organizations know that their initial suspicions have some validity. Moreover, the process must support notification of all ISE participants when further evidence determines that an ISE-SAR was designated incorrectly so that the original information does not continue to be used as the basis for analysis or action. This type of feedback can support organizational redress processes and procedures where appropriate.

E. Broader ISE-SAR Applicability

Consistent with the ISE Privacy Guidelines and Presidential Guideline 2, and to the full extent permitted by law, this *ISE-SAR Functional Standard* is designed to support the sharing of unclassified information or sensitive but unclassified (SBU)/controlled unclassified information (CUI) within the ISE. There is also a provision for using a data element indicator for designating classified national security information as part of the ISE-SAR record, as necessary. This condition could be required under special circumstances for protecting the context of the event, or specifics or organizational associations of affected locations. The State or major urban area fusion center shall act as the key conduit between the State, local, and tribal (SLT) agencies and other ISE participants. It is also important to note that the ISE Shared Spaces implementation concept is focused exclusively on terrorism-related information. However many SAR originators and consumers have responsibilities beyond terrorist activities. Of special note, there is no intention to modify or otherwise affect, through this *ISE-SAR Functional Standard*, the currently supported or mandated direct interactions between State, local, and tribal law enforcement and investigatory personnel and the Joint Terrorism Task Forces (JTTFs) or Field Intelligence Groups (FIGs).

This *ISE-SAR Functional Standard* will be used as the ISE-SAR information exchange standard for all ISE participants. Although the extensibility of this *ISE-SAR Functional Standard* does support customization for unique communities, jurisdictions planning to modify this *ISE-SAR Functional Standard* must carefully consider the consequences of customization. The PM-ISE requests that modification follow a formal change request process through the ISE-SAR Steering Committee and CTISS Committee under the Information Sharing Council, for both community coordination and consideration. Furthermore, messages that do not conform to this Functional Standard may not be consumable by the receiving organization and may require modifications by the nonconforming organizations.

---

[10] The Reevaluation Phase also encompasses the establishment of an integrated counterterrorism information needs process, a process that does not relate directly to information exchanges through this standard. See page 23 of the *NSI CONOPS* for more details.

F. Protecting Privacy

Laws that prohibit or otherwise limit the sharing of personal information vary considerably between the Federal, State, local, and tribal levels. The Privacy Act of 1974 (5 USC §552a) as amended, other statutes such as the E-Government Act, and many government-wide or departmental regulations establish a framework and criteria for protecting information privacy in the Federal Government. The ISE must facilitate the sharing of information in a lawful manner, which by its nature must recognize, in addition to Federal statutes and regulations, different State, local or tribal laws, regulations, or policies that affect privacy. One method for protecting privacy while enabling the broadest possible sharing is to anonymize ISE-SAR reports by excluding data elements that contain personal information. Accordingly, two different formats are available for ISE-SAR information. The **Detailed ISE-SAR IEPD** format includes personal information contained in the data fields set forth in Section IV of this *ISE-SAR Functional Standard* ("ISE-SAR Exchange Data Model"), including "privacy fields" denoted as containing personal information. If an ISE participant is not authorized to disseminate personal information from an ISE Shared Space (e.g., the requester site does not have a compliant privacy policy) or the SAR does not evidence the necessary nexus to terrorism-related crime (as required by this *ISE-SAR Functional Standard*), information from the privacy fields will not be loaded into the responsive document (search results) from the ISE Shared Space. This personal information will not be passed to the ISE participant. The **Summary ISE-SAR Information** format excludes privacy fields or data elements identified in Section IV of this *ISE-SAR Functional Standard* as containing personal information. Each ISE participant can exclude additional data elements from the **Summary ISE-SAR Information** format in accordance with its own legal and policy requirements. It is believed the data contained within a **Summary ISE-SAR Information** format will support sufficient trending and pattern recognition to trigger further analysis and/or investigation where additional information can be requested from the sending organization. Because of variances of data expected within ISE-SAR exchanges, only the minimum elements are considered mandatory. These are enumerated in the READ ME document in the technical artifacts folder that is part of this *ISE-SAR Functional Standard*.

Currently, the privacy fields identified in the ISE-SAR exchange data model (Section IV, below) are the minimum fields that should be removed from a **Detailed ISE-SAR IEPD**.

SECTION III – INFORMATION EXCHANGE DEVELOPMENT

This *ISE-SAR Functional Standard* is a collection of artifacts that support an implementer's creation of ISE-SAR information exchanges, whether **Detailed ISE-SAR IEPD** or **Summary ISE-SAR Information**. The basic ISE-SAR information exchange is documented using five unique artifacts giving implementers tangible products that can be leveraged for local implementation. A domain model provides a graphical depiction of those data elements required for implementing an exchange and the cardinality between those data elements. Second, a Component Mapping Template is a spreadsheet that associates each required data element with its corresponding XML data element. Third, information exchanges include the schemas which consist of a document, extension, and constraint schema. Fourth, at least one sample XML Instance and associated style-sheet is included to help practitioners validate the model, mapping, and schemas in a more intuitive way. Fifth, a codified data field values listing provides listings, descriptions, and sources as prescribed by the data fields.

SECTION IV – ISE-SAR EXCHANGE DATA MODEL

A. Summary of Elements

This section contains a full inventory of all ISE-SAR information exchange data classes, elements, and definitions. Items and definitions contained in cells with a light purple background are data classes, while items and definition contained in cells with a white background are data elements. A wider representation of data class and element mappings to source (ISE-SAR information exchange) and target is contained in the Component Mapping Template located in the technical artifacts folder.

Cardinality between objects in the model is indicated on the line in the domain model (see Section 5A). Cardinality indicates how many times an entity can occur in the model. For example, Vehicle, Vessel, and Aircraft all have cardinality of 0..n. This means that they are optional, but may occur multiple times if multiple suspect vehicles are identified.

Clarification of Organizations used in the exchange:

- The **Source Organization** is the agency or entity that originates the SAR report (examples include a local police department, a private security firm handling security for a power plant, and a security force at a military installation). The Source Organization will not change throughout the life of the SAR.
- The **Submitting Organization** is the organization providing the ISE-SAR to the community through their ISE Shared Space. The Submitting Organization and the Source Organization may be the same.
- The **Owning Organization** is the organization that owns the target associated with the suspicious activity.

Table 2 – ISE-SAR Information Exchange Data Classes, Elements, and Definitions

Privacy Field	Source Class/Element	Source Definition
	Aircraft	
	Aircraft Engine Quantity	The number of engines on an observed aircraft.
	Aircraft Fuselage Color	A code identifying a color of a fuselage of an aircraft.
	Aircraft Wing Color	A code identifying a color of a wing of an aircraft.
X	Aircraft ID	A unique identifier assigned to the aircraft by the observing organization—used for referencing. *If this identifier can be used to identify a specific aircraft, for instance, by using the aircraft tail number, then this element is a privacy field. [free text field]
	Aircraft Make Code	A code identifying a manufacturer of an aircraft.
	Aircraft Model Code	A code identifying a specific design or type of aircraft made by a manufacturer.

Privacy Field	Source Class/Element	Source Definition
	Aircraft Style Code	A code identifying a style of an aircraft.
X	Aircraft Tail Number	An aircraft identification number prominently displayed at various locations on an aircraft, such as on the tail and along the fuselage. [free text field]
	Attachment	
	Attachment Type Text	Describes the type of attachment (e.g., surveillance video, mug shot, evidence). [free text field]
	Binary Image	Binary encoding of the attachment.
	Capture Date	The date that the attachment was created.
	Description Text	Text description of the attachment. [free text field]
	Format Type Text	Format of attachment (e.g., mpeg, jpg, avi). [free text field]
	Attachment URI	Uniform Resource Identifier (URI) for the attachment. Used to match the attachment link to the attachment itself. Standard representation type that can be used for Uniform Resource Locators (URLs) and Uniform Resource Names (URNs).
	Attachment Privacy Field Indicator	Identifies whether the binary attachment contains information that may be used to identify an individual.
	Contact Information	
	Person First Name	Person to contact at the organization.
	Person Last Name	Person to contact at the organization.
	E-Mail Address	An email address of a person or organization. [free text field]
	Full Telephone Number	A full length telephone identifier representing the digits to be dialed to reach a specific telephone instrument. [free text field]
	Driver License	
X	Expiration Date	The month, date, and year that the document expires.
	Expiration Year	The year the document expires.
	Issuing Authority Text	Code identifying the organization that issued the driver license assigned to the person. Examples include Department of Motor Vehicles, Department of Public Safety and Department of Highway Safety and Motor Vehicles. [free text field]
X	Driver License Number	A driver license identifier or driver license permit identifier of the observer or observed person of interest involved with the suspicious activity. [free text field]
	Follow-Up Action	
	Activity Date	Date that the follow-up activity started.
	Activity Time	Time that the follow up activity started.
	Assigned By Text	Organizational identifier that describes the organization performing a follow-up activity. This is designed to keep all parties interested in a particular ISE-SAR informed of concurrent investigations. [free text field]
	Assigned To Text	Text describing the person or sub-organization that will be performing the designated action. [free text field]
	Disposition Text	Description of disposition of suspicious activity investigation. [free text field]
	Status Text	Description of the state of follow-up activity. [free text field]
	Location	

Privacy Field	Source Class/Element	Source Definition
X	Location Description	A description of a location where the suspicious activity occurred. If the location is an address that is not broken into its component parts (e.g., 1234 Main Street), this field may be used to store the compound address. [free text field]
	Location Address	
	Building Description	A complete reference that identifies a building. [free text field]
	County Name	A name of a county, parish, or vicinage. [free text field]
	Country Name	A country name or other identifier. [free text field]
	Cross Street Description	A description of an intersecting street. [free text field]
	Floor Identifier	A reference that identifies an actual level within a building. [free text field]
	ICAO Airfield Code for Departure	An International Civil Aviation Organization (ICAO) airfield code for departure, indicates aircraft, crew, passengers, and cargo-on conveyance location information. [free text field]
	ICAO Airfield Code for Planned Destination	An airfield code for planned destination, indicates aircraft, crew, passengers, and cargo on conveyance location information [free text field]
	ICAO for Actual Destination	An airfield code for actual destination. Indicates aircraft, crew, passengers, and cargo on conveyance location information. [free text field]
	ICAO Airfield for Alternate	An airfield code for Alternate. Indicates aircraft, crew, passengers, and cargo on conveyance location information. [free text field]
	Mile Marker Text	Identifies the sequentially numbered marker on a roadside that is closest to the intended location. Also known as milepost, or mile post. [free text field]
	Municipality Name	The name of the city or town. [free text field]
	Postal Code	The zip code or postal code. [free text field]
	State Name	Code identifying the state.
	Street Name	A name that identifies a particular street. [free text field]
X	Street Number	A number that identifies a particular unit or location within a street. [free text field]
	Street Post Directional	A direction that appears after a street name. [free text field]
	Street Pre Directional	A direction that appears before a street name. [free text field]
	Street Type	A type of street, e.g., Street, Boulevard, Avenue, Highway. [free text field]
X	Unit ID	A particular unit within the location. [free text field]
	Location Coordinates	
	Altitude	Height above or below sea-level of a location.
	Coordinate Datum	Coordinate system used for plotting location.
	Latitude Degree	A value that specifies the degree of a latitude. The value comes from a restricted range between -90 (inclusive) and +90 (inclusive).
	Latitude Minute	A value that specifies a minute of a degree. The value comes from a restricted range of 0 (inclusive) to 60 (exclusive).
	Latitude Second	A value that specifies a second of a minute. The value comes from a restricted range of 0 (inclusive) to 60 (exclusive).

Privacy Field	Source Class/Element	Source Definition
	Longitude Degree	A value that specifies the degree of a longitude. The value comes from a restricted range between -180 (inclusive) and +180 (exclusive).
	Longitude Minute	A value that specifies a minute of a degree. The value comes from a restricted range of 0 (inclusive) to 60 (exclusive).
	Longitude Second	A value that specifies a second of a minute. The value comes from a restricted range of 0 (inclusive) to 60 (exclusive).
	Conveyance track/intent	A direction by heading and speed or enroute route and/or waypoint of conveyance [free text field]
	Observer	
	Observer Type Text	Indicates the relative expertise of an observer to the suspicious activity (e.g., professional observer versus layman). Example: a security guard at a utility plant recording the activity, or a citizen driving by viewing suspicious activity. [free text field]
X	Person Employer ID	Number assigned by an employer for a person such as badge number. [free text field]
	Owning Organization	
	Organization Item	A name of an organization that owns the target. [free text field]
	Organization Description	A text description of organization that owns the target. The description may indicate the type of organization such as State Bureau of Investigation, Highway Patrol, etc. [free text field]
X	Organization ID	A federal tax identifier assigned to an organization. Sometimes referred to as a Federal Employer Identification Number (FEIN), or an Employer Identification Number (EIN). [free text field]
	Organization Local ID	An identifier assigned on a local level to an organization. [free text field]
	Other Identifier	
X	Person Identification Number (PID)	An identifying number assigned to the person, e.g., military serial numbers. [free text field]
X	PID Effective Date	The month, date, and year that the PID number became active or accurate.
	PID Effective Year	The year that the PID number became active or accurate.
X	PID Expiration Date	The month, date, and year that the PID number expires.
	PID Expiration Year	The year that the PID number expires.
	PID Issuing Authority Text	The issuing authority of the identifier. This may be a State, military organization, etc.
	PID Type Code	Code identifying the type of identifier assigned to the person. [free text field]
	Passport	
X	Passport ID	Document Unique Identifier. [free text field]
X	Expiration Date	The month, date, and year that the document expires.
	Expiration Year	The year the document expires.
	Issuing Country Code	Code identifying the issuing country. [free text field]
	Person	
X	AFIS FBI Number	A number issued by the FBI's Automated Fingerprint Identification System (AFIS) based on submitted fingerprints. [free text field]

Privacy Field	Source Class/Element	Source Definition
	Age	A precise measurement of the age of a person.
	Age Unit Code	Code that identifies the unit of measure of an age of a person (e.g., years, months). [free text field]
X	Date of Birth	The month, date, and year that a person was born.
	Year of Birth	The year a person was born.
	Ethnicity Code	Code that identifies the person's cultural lineage.
	Maximum Age	The maximum age measurement in an estimated range.
	Minimum Age	The minimum age measurement in an estimated range.
X	State Identifier	Number assigned by the State based on biometric identifiers or other matching algorithms. [free text field]
X	Tax Identifier Number	A 9-digit numeric identifier assigned to a living person by the U.S. Social Security Administration. A social security number of the person. [free text field]
	Person Name	
X	First Name	A first name or given name of the person. [free text field]
X	Last Name	A last name or family name of the person. [free text field]
X	Middle Name	A middle name of a person. [free text field]
X	Full Name	Used to designate the compound name of a person that includes all name parts. This field should only be used when the name cannot be broken down into its component parts or if the information is not available in its component parts. [free text field]
X	Moniker	Alternative, or gang name for a person. [free text field]
	Name Suffix	A component that is appended after the family name that distinguishes members of a family with the same given, middle, and last name, or otherwise qualifies the name. [free text field]
	Name Type	Text identifying the type of name for the person. For example, maiden name, professional name, nick name.
	Physical Descriptors	
	Build Description	Text describing the physique or shape of a person. [free text field]
	Eye Color Code	Code identifying the color of the person's eyes.
	Eye Color Text	Text describing the color of a person's eyes. [free text field]
	Hair Color Code	Code identifying the color of the person's hair.
	Hair Color Text	Text describing the color of a person's hair. [free text field]
	Person Eyewear Text	A description of glasses or other eyewear a person wears. [free text field]
	Person Facial Hair Text	A kind of facial hair of a person. [free text field]
	Person Height	A measurement of the height of a person.
	Person Height Unit Code	Code that identifies the unit of measure of a height of a person. [free text field]
	Person Maximum Height	The maximum measure value on an estimated range of the height of the person.
	Person Minimum Height	The minimum measure value on an estimated range of the height of the person.
	Person Maximum Weight	The maximum measure value on an estimated range of the weight of the person.

Privacy Field	Source Class/Element	Source Definition
	Person Minimum Weight	The minimum measure value on an estimated range of the weight of the person.
	Person Sex Code	A code identifying the gender or sex of a person (e.g., Male or Female).
	Person Weight	A measurement of the weight of a person.
	Person Weight Unit Code	Code that identifies the unit of measure of a weight of a person. [free text field]
	Race Code	Code that identifies the race of the person.
	Skin Tone Code	Code identifying the color or tone of a person's skin.
	Clothing Description Text	A description of an article of clothing. [free text field]
	Physical Feature	
	Feature Description	A text description of a physical feature of the person. [free text field]
	Feature Type Code	A special kind of physical feature or any distinguishing feature. Examples include scars, marks, tattoos, or a missing ear. [free text field]
	Location Description	A description of a location. If the location is an address that is not broken into its component parts (e.g., 1234 Main Street), this field may be used to store the compound address. [free text field]
	Registration	
	Registration Authority Code	Text describing the organization or entity authorizing the issuance of a registration for the vehicle involved with the suspicious activity. [free text field]
X	Registration Number	The number on a metal plate fixed to/assigned to a vehicle. The purpose of the registration number is to uniquely identify each vehicle within a state. [free text field]
	Registration Type	Code that identifies the type of registration plate or license plate of a vehicle. [free text field]
	Registration Year	A 4-digit year as shown on the registration decal issued for the vehicle.
	ISE-SAR Submission	
	Additional Details Indicator	Identifies whether more ISE-SAR details are available at the authoring/originating agency than what has been provided in the information exchange.
	Data Entry Date	Date the data was entered into the reporting system (e.g., the Records Management System).
	Dissemination Code	Generally established locally, this code describes the authorized recipients of the data. Examples include Law Enforcement Use, Do Not Disseminate, etc.
	Fusion Center Contact First Name	Identifies the first name of the person to contact at the fusion center. [free text field]
	Fusion Center Contact Last Name	Identifies the last name of the person to contact at the fusion center. [free text field]
	Fusion Center Contact E-Mail Address	Identifies the email address of the person to contact at the fusion center. [free text field]
	Fusion Center Contact Telephone Number	The full phone number of the person at the fusion center that is familiar with the record (e.g., law enforcement officer).

Privacy Field	Source Class/Element	Source Definition
	Message Type Indicator	e.g., Add, Update, Purge.
	Privacy Purge Date	The date by which the privacy information will be purged from the record system; general observation data is retained.
	Privacy Purge Review Date	Date of review to determine the disposition of the privacy fields in a Detailed ISE-SAR IEPD record.
	Submitting ISE-SAR Record ID	Identifies the Fusion Center ISE-SAR Record identifier for reports that are possibly related to the current report. [free text field]
	ISE-SAR Submission Date	Date of submission for the ISE-SAR Record.
	ISE-SAR Title	Plain language title (e.g., Bomb threat at the "X" Hotel). [free text field]
	ISE-SAR Version	Indicates the specific version of the ISE-SAR that the XML Instance corresponds. [free text field]
	Source Agency Case ID	The case identifier for the agency that originated the SAR. Often, this will be a local law enforcement agency. [free text field]
	Source Agency Record Reference Name	The case identifier that is commonly used by the source agency—may be the same as the System ID. [free text field]
	Source Agency Record Status Code	The current status of the record within the source agency system.
	Privacy Information Exists Indicator	Indicates whether privacy information is available from the source fusion center. This indicator may be used to guide people who only have access to the summary information exchange as to whether or not they can follow-up with the originating fusion center to obtain more information.
	Sensitive Information Details	
	Classification Label	A classification of information. Includes Confidential, Secret, Top Secret, no markings. [free text field]
	Classification Reason Text	A reason why the classification was made as such. [free text field]
	Sensitivity Level	Local information security categorization level (Controlled Unclassified Information-CUI, including Sensitive But Unclassified or Law Enforcement Sensitive). [free text field]
	Tearlined Indicator	Identifies whether a report is free of classified information.
	Source Organization	
	Organization Name	The name used to refer to the agency originating the SAR. [free text field]
	Organization ORI	Originating Agency Identification (ORI) used to refer to the agency.
	System ID	The system that the case identifier (e.g., Records Management System, Computer Aided Dispatch) relates to within or the organization that originated the Suspicious Activity Report. [free text field]
	Fusion Center Submission Date	Date of submission to the Fusion Center.
	Source Agency Contact First Name	The first name of the person at the agency that is familiar with the record (e.g., law enforcement officer). [free text field]
	Source Agency Contact Last Name	The last name of the person at the agency that is familiar with the record (e.g., law enforcement officer). [free text field]
	Source Agency Contact Email Address	The email address of the person at the agency that is familiar with the record (e.g., law enforcement officer). [free text field]

Privacy Field	Source Class/Element	Source Definition
	Source Agency Contact Phone Number	The full phone number of the person at the agency that is familiar with the record (e.g., law enforcement officer).
	Suspicious Activity Report	
	Community Description	Describes the intended audience of the document. [free text field]
	Community URI	The URL to resolve the ISE-SAR information exchange payload namespace.
	LEXS Version	Identifies the version of Department of Justice LEISP Exchange Specification (LEXS) used to publish this document. ISE-FS-200 has been built using LEXS version 3.1. The schema was developed by starting with the basic LEXS schema and extending that definition by adding those elements not included in LEXS. [free text field]
	Message Date/Time	A timestamp identifying when this message was received.
	Sequence Number	A number that uniquely identifies this message.
	Source Reliability Code	Reliability of the source, in the assessment of the reporting organization: could be one of 'reliable', 'unreliable', or 'unknown'
	Content Validity Code	Validity of the content, in the assessment of the reporting organization: could be one of 'confirmed', 'doubtful', or 'cannot be judged'
	Nature of Source-Code	Nature of the source: Could be one of 'anonymous tip', 'confidential source', trained interviewer', 'written statement – victim, witness, other', private sector', or 'other source'
	Nature of Source-Text	Optional information of 'other source' is selected above. [free text field]
	Submitting Organization	
	Organization Name	Common Name of the fusion center or ISE participant that submitted the ISE-SAR record to the ISE. [free text field]
	Organization ID	Fusion center or ISE participant's alpha-numeric identifier. [free text field]
	Organization ORI	ORI for the submitting fusion center or ISE participant. [free text field]
	System ID	Identifies the system within the fusion center or ISE participant that is submitting the ISE-SAR. [free text field]
	Suspicious Activity	
	Activity End Date	The end or completion date in Greenwich Mean Time (GMT) of an incident that occurs over a duration of time.
	Activity End Time	The end or completion time in GMT of day of an incident that occurs over a duration of time.
	Activity Start Date	The date in GMT when the incident occurred or the start date if the incident occurs over a period of time.
	Activity Start Time	The time of day in GMT that the incident occurred or started.
	Observation Description Text	Description of the activity including rational for potential terrorism nexus. [free text field]
	Observation End Date	The end or completion date in GMT of the observation of an activity that occurs over a duration of time.
	Observation End Time	The end or completion time of day in GMT of the observation of an activity that occurred over a period of time.

Privacy Field	Source Class/Element	Source Definition
	Observation Start Date	The date in GMT when the observation of an activity occurred or the start date if the observation of the activity occurred over a period of time.
	Observation Start Time	The time of day in GMT that the observation of an activity occurred or started.
	Threat Type Code	Broad category of threat to which the tip or lead pertains. Includes Financial Incident, Suspicious Activity, and Cyber Crime.
	Threat Type Detail Text	Breakdown of the Tip Type, it indicates the type of threat to which the tip or lead pertains. The subtype is often dependent on the Tip Type. For example, the subtypes for a nuclear/radiological tip class might be Nuclear Explosive or a Radiological Dispersal Device. [free text field]
	Suspicious Activity Code	Indicates the type of threat to which the tip or lead pertains. Examples include a biological or chemical threat.
	Weather Condition Details	The weather at the time of the suspicious activity. The weather may be described using codified lists or text.
	Target	
	Critical Infrastructure Indicator	Critical infrastructure, as defined by 42 USC Sec. 5195c, means systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.
	Infrastructure Sector Code	The broad categorization of the infrastructure type. These include telecommunications, electrical power systems, gas and oil storage and transportation, banking and finance, transportation, water supply systems, emergency services (including medical, police, fire, and rescue), and continuity of government.
	Infrastructure Tier Text	Provides additional detail that enhances the Target Sector Code. For example, if the target sector is Utilities, this field would indicate the type of utility that has been targeted such as power station or power transmission. [free text field]
	Structure Type Code	National Data Exchange (N-DEx) Code that identifies the type of Structure that was involved in the incident.
	Target Type Text	Describes the target type if an appropriate sector code is not available. [free text field]
	Structure Type Text	Text for use when the Structure Type Code does not afford necessary code. [free text field]
	Target Description Text	Text describing the target (e.g., Lincoln Bridge). [free text field]
	Vehicle	
	Color Code	Code that identifies the primary color of a vehicle involved in the suspicious activity.
	Description	Text description of the entity. [free text field]
	Make Name	Code that identifies the manufacturer of the vehicle.
	Model Name	Code that identifies the specific design or type of vehicle made by a manufacturer—sometimes referred to as the series model.
	Style Code	Code that identifies the style of a vehicle. [free text field]
	Vehicle Year	A 4-digit year that is assigned to a vehicle by the manufacturer.

Privacy Field	Source Class/Element	Source Definition
X	Vehicle Identification Number	Used to uniquely identify motor vehicles. [free text field]
X	US DOT Number	An assigned number sequence required by Federal Motor Carrier Safety Administration (FMCSA) for all interstate carriers. The identification number (found on the power unit, and assigned by the U.S. Department of Transportation or by a State) is a key element in the FMCSA databases for both carrier safety and regulatory purposes. [free text field]
	Vehicle Description	A text description of a vehicle. Can capture unique identifying information about a vehicle such as damage, custom paint, etc. [free text field]
	Related ISE-SAR	
	Fusion Center ID	Identifies the fusion center that is the source of the ISE-SAR. [free text field]
	Fusion Center ISE-SAR Record ID	Identifies the fusion center ISE-SAR record identifier for reports that are possibly related to the current report.
	Relationship Description Text	Describes how this ISE-SAR is related to another ISE-SAR. [free text field]
	Vessel	
X	Vessel Official Coast Guard Number Identification	An identification for the Official (U.S. Coast Guard Number of a vessel). Number is encompassed within valid marine documents and permanently marked on the main beam of a documented vessel. [free text field]
X	Vessel ID	A unique identifier assigned to the boat record by the agency—used for referencing. [free text field]
	Vessel ID Issuing Authority	Identifies the organization authorization over the issuance of a vessel identifier. Examples of this organization include the State Parks Department and the Fish and Wildlife department. [free text field]
X	Vessel IMO Number Identification	An identification for an International Maritime Organization Number (IMO number) of a vessel [free text field]
	Vessel MMSI Identification	An identification for the Maritime Mobile Service Identity (MMSI) or a vessel [free text field]
	Vessel Make	Code that identifies the manufacturer of the boat.
	Vessel Model	Model name that identifies the specific design or type of boat made by a manufacturer—sometimes referred to as the series model.
	Vessel Model Year	A 4-digit year that is assigned to a boat by the manufacturer.
	Vessel Name	Complete boat name and any numerics. [free text field]
	Vessel Hailing Port	The identifying attributes of the hailing port of a vessel [free text field]
	Vessel National Flag	A data concept for a country under which a vessel sails. [free text field]
	Vessel Overall Length	The length measurement of the boat, bow to stern.
	Vessel Overall Length Measure	Code that identifies the measurement unit used to determine the boat length. [free text field]
X	Vessel Serial Number	The identification number of a boat involved in an incident. [free text field]
	Vessel Type Code	Code that identifies the type of boat.

Privacy Field	Source Class/Element	Source Definition
	Vessel Propulsion Text	Text for use when the Boat Propulsion Code does not afford necessary code. [free text field]

B. Association Descriptions

This section defines specific data associations contained in the ISE-SAR data model structure. Reference Figure 2 (UML-based model) for the graphical depiction and detailed elements.

Table 3 – ISE-SAR Data Model Structure Associations

Link Between Associated Components	Target Element
Link From Suspicious Activity Report to Attachment	lexs:Digest/lexsdigest:Associations/lexsdigest:EntityAttachmentLinkAssociation
Link From Suspicious Activity Report to Sensitive Information Details	Hierarchical Association
Link From Suspicious Activity Report to ISE-SAR Submission	Hierarchical Association
Link From Suspicious Activity to Vehicle	lexs:Digest/lexsdigest:Associations/lexsdigest:IncidentInvolvedItemAssociation
Link From Vehicle to Registration	Hierarchical Association
Link From Suspicious Activity to Vessel	lexs:Digest/lexsdigest:Associations/lexsdigest:IncidentInvolvedItemAssociation
Link From Suspicious Activity to Aircraft	lexs:Digest/lexsdigest:Associations/lexsdigest:IncidentInvolvedItemAssociation
Link From Suspicious Activity to Location	lexs:Digest/lexsdigest:Associations/lexsdigest:ActivityLocationAssociation
Link From Suspicious Activity to Target	Hierarchical Association
Link From Location to Location Coordinates	Hierarchical Association
Link From Location to Location Address	Hierarchical Association
Link From Suspicious Activity Report to Related ISE-SAR	Hierarchical Association
Link From Person to Location	lexs:Digest/lexsdigest:Associations/lexsdigest:PersonLocationAssociation
Link From Person to Contact Information	lexs:Digest/lexsdigest:Associations/lexsdigest:EntityEmailAssociation or lexs:Digest/lexsdigest:Associations/lexsdigest:EntityTelephoneNumberAssociation
Link From Person to Driver License	Hierarchical Association
Link From Person to Passport	Hierarchical Association
Link From Person to Other Identifier	Hierarchical Association

Link Between Associated Components	Target Element
Link From Person to Physical Descriptors	Hierarchical Association
Link From Person to Physical Feature	Hierarchical Association
Link From Person to Person Name	Hierarchical Association
Link From Suspicious Activity Report to Follow-Up Action	Hierarchical Association
Link From Target to Location	lexs:Digest/lexsdigest:Associations/lexsdigest:ItemLocationAssociation
Link From Suspicious Activity Report to Organization	Hierarchical Association
Link From Suspicious Activity to Person [Witness]	lexs:Digest/lexsdigest:Associations/lexsdigest:IncidentWitnessAssociation
Link From Suspicious Activity to Person [Person Of Interest]	lexs:Digest/lexsdigest:Associations/lexsdigest:PersonOfInterestAssociation
Link From Organization to Target	ext:SuspiciousActivityReport/nc:OrganizationItemAssociation
Link from ISE-SAR Submission to Submitting Organization	Hierarchical Association
Link From Submitting Organization to Contact Information	Hierarchical Association (Note that the mapping indicates context and we are not reusing Contact Information components)

C. Extended XML Elements

Additional data elements are also identified as new elements outside of NIEM, Version 2.0. These elements are listed below:

AdditionalDetailsIndicator: Identifies whether more ISE-SAR details are available at the authoring/originating agency than what has been provided in the information exchange.

AssignedByText: Organizational identifier that describes the organization performing a follow-up activity. This is designed to keep all parties interested in a particular ISE-SAR informed of concurrent investigations.

AssignedToText: Text describing the person or sub-organization that will be performing the designated follow-up action.

ClassificationReasonText: A reason why the classification was made as such.

ContentValidityCode: Validity of the content, in the assessment of the reporting organization: could be one of ‘confirmed’, ‘doubtful’, or ‘cannot be judged’.

Conveyancetrack/intent: A direction by heading and speed or enroute route and/or waypoint of conveyance.

CriticalInfrastructureIndicator: Critical infrastructure, as defined by 42 USC Sec. 5195c, means systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.

ICAOAirfieldCodeforDeparture: An International Civil Aviation Organization (ICAO) airfield code for departure, indicates aircraft, crew, passengers, and cargo-on conveyance location information.

ICAOAirfieldCodeforPlannedDestination: An airfield code for planned destination, indicates aircraft, crew, passengers, and cargo on conveyance location information.

ICAOforActualDestination: An airfield code for actual destination. Indicates aircraft, crew, passengers, and cargo on conveyance location information.

ICAOAirfieldforAlternate: An airfield code for Alternate. Indicates aircraft, crew, passengers, and cargo on conveyance location information.

NatureofSource-Code: Nature of the source: Could be one of ‘anonymous tip’, ‘confidential source’, trained interviewer’, ‘written statement – victim, witness, other’, private sector’, or ‘other source’.

PrivacyFieldIndicator: Data element that may be used to identify an individual and therefore is subject to protection from disclosure under applicable privacy rules. Removal of privacy fields from a detailed report will result in a summary report. This privacy field informs users of the summary information exchange that additional information may be available from the originator of the report.

ReportPurgeDate: The date by which the privacy fields will be purged from the record system; general observation data is retained. Purge policies vary from jurisdiction to jurisdiction and should be indicated as part of the guidelines.

ReportPurgeReviewDate: Date of review to determine the disposition of the privacy fields in a Detailed ISE-SAR IEPD record.

SourceReliabilityCode: Reliability of the source, in the assessment of the reporting organization: could be one of ‘reliable’, ‘unreliable’, or ‘unknown’.

VesselHailingPort: The identifying attributes of the hailing port of a vessel.

VesselNationalFlag: A data concept for a country under which a vessel sails.

SECTION V – INFORMATION EXCHANGE IMPLEMENTATION ARTIFACTS

A. Domain Model

1. General Domain Model Overview

The domain model provides a visual representation of the business data requirements and relationships (Figure 2). This Unified Modeling Language (UML)-based Model represents the Exchange Model artifact required in the information exchange development methodology. The model is designed to demonstrate the organization of data elements and illustrate how these elements are grouped together into Classes. Furthermore, it describes relationships between these Classes. A key consideration in the development of a Domain Model is that it must be independent of the mechanism intended to implement the model. The domain model is actually a representation of how data is structured from a *business* context. As the technology changes and new Functional Standards emerge, developers can create new standards mapping documents and schema tied to a new standard without having to re-address business process requirements.

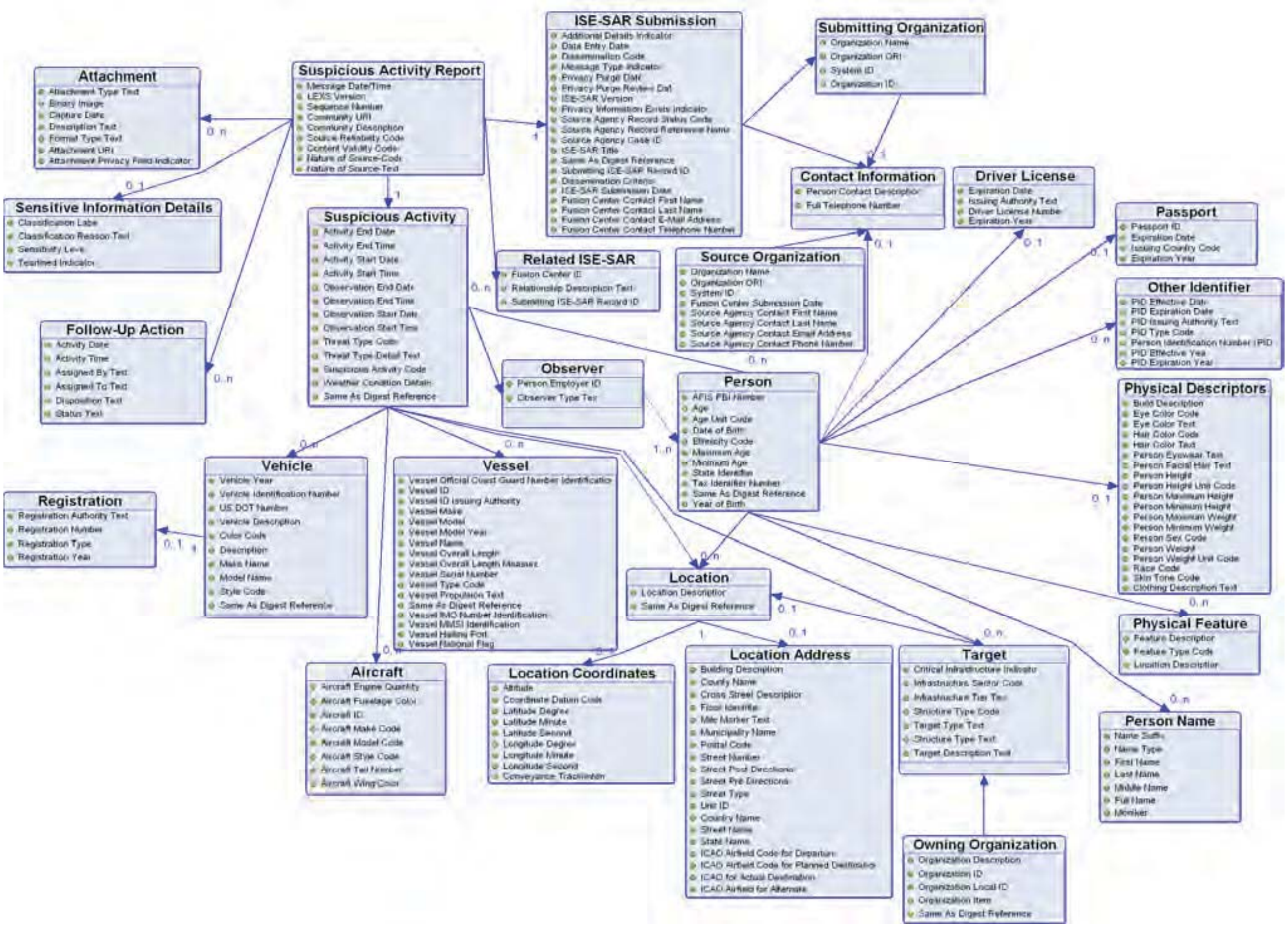

ISE-SAR Submission
Submitting Organization
Attachment
Suspicious Activity Report
Sensitive Information Details
Suspicious Activity
Contact Information
Driver License
Passport
Related ISE-SAR
Source Organization
Other Identifier
Follow-Up Action
Observer
Person
Physical Descriptors
Vehicle
Vessel
Registration
Location
Physical Feature
Aircraft
Location Coordinates
Location Address
Target
Person Name
Owning Organization

Figure 2 – UML-based Model

B. General Mapping Overview

The detailed component mapping template provides a mechanism to cross-reference the business data requirements documented in the Domain Model to their corresponding XML Element in the XML Schema. It includes a number of items to help establish equivalency including the business definition and the corresponding XML Element Definition.

C. ISE-SAR Mapping Overview

The Mapping Spreadsheet contains seven unique items for each ISE-SAR data class and element. The Mapping Spreadsheet columns are described in this section.

Table 4 – Mapping Spreadsheet Column Descriptions

Spreadsheet Name & Row	Description
Privacy Field Indicator	This field indicates that the information may be used to identify an individual.
Source Class/ Element	Content in this column is either the data class (grouping of data elements) or the actual data elements. Classes are highlighted and denoted with cells that contain blue background while elements have a white background. The word "Source" is referring to the ISE-SAR information exchange.
Source Definition	The content in this column is the class or element definition defined for this ISE-SAR information exchange. The word "Source" is referring to the ISE-SAR information exchange definition.
Target Element	The content in this column is the actual namespace path deemed equal to the related ISE-SAR information exchange element.
Target Element Definition	The content in this column provides the definition of the target or NIEM element located at the aforementioned source path. "Target" is referring to the NIEM definition.
Target Element Base	Indicates the data type of the terminal element. Data types of niem-xsd:String or nc:TextType indicate free-form text fields.
Mapping Comments	Provides technical implementation information for developers and implementers of the information exchange.

D. Schemas

The *ISE-SAR Functional Standard* contains the following compliant schemas;

- Subset Schema
- Exchange Schema
- Extension Schema
- Wantlist

E. Examples

The *ISE-SAR Functional Standard* contains two samples that illustrate exchange content as listed below.

1. XSL Style Sheet

This information exchange artifact provides an implementer and users with a communication tool which captures the look and feel of a familiar form, screen, or like peripheral medium for schema translation testing and user validation of business rules.

2. XML Instance

This information exchange artifact provides an actual payload of information with data content defined by the schema(s).

PART B – ISE-SAR CRITERIA GUIDANCE

Category	Description
DEFINED CRIMINAL ACTIVITY AND POTENTIAL TERRORISM NEXUS ACTIVITY	
Breach/Attempted Intrusion	Unauthorized personnel attempting to or actually entering a restricted area or protected site. Impersonation of authorized personnel (e.g. police/security, janitor).
Misrepresentation	Presenting false or misusing insignia, documents, and/or identification, to misrepresent one's affiliation to cover possible illicit activity.
Theft/Loss/Diversion	Stealing or diverting something associated with a facility/infrastructure (e.g., badges, uniforms, identification, emergency vehicles, technology or documents {classified or unclassified}, which are proprietary to the facility).
Sabotage/Tampering/ Vandalism	Damaging, manipulating, or defacing part of a facility/infrastructure or protected site.
Cyber Attack	Compromising, or attempting to compromise or disrupt an organization's information technology infrastructure.
Expressed or Implied Threat	Communicating a spoken or written threat to damage or compromise a facility/infrastructure.
Aviation Activity	Operation of an aircraft in a manner that reasonably may be interpreted as suspicious, or posing a threat to people or property. Such operation may or may not be a violation of Federal Aviation Regulations.
POTENTIAL CRIMINAL OR NON-CRIMINAL ACTIVITY REQUIRING ADDITIONAL FACT INFORMATION DURING INVESTIGATION[11]	
Eliciting Information	Questioning individuals at a level beyond mere curiosity about particular facets of a facility's or building's purpose, operations, security procedures, etc., that would arouse suspicion in a reasonable person.
Testing or Probing of Security	Deliberate interactions with, or challenges to, installations, personnel, or systems that reveal physical, personnel or cyber security capabilities.
Recruiting	Building of operations teams and contacts, personnel data, banking data or travel data
Photography	Taking pictures or video of facilities, buildings, or infrastructure in a manner that would arouse suspicion in a reasonable person. Examples include taking pictures or video of infrequently used access points, personnel performing security functions (patrols, badge/vehicle checking), security-related equipment (perimeter fencing, security cameras), etc.

[11] Note: These activities are generally First Amendment-protected activities and should not be reported in a SAR or ISE-SAR absent articulable facts and circumstances that support the source agency's suspicion that the behavior observed is not innocent, but rather reasonably indicative of criminal activity associated with terrorism, including evidence of pre-operational planning related to terrorism. Race, ethnicity, national origin, or religious affiliation should not be considered as factors that create suspicion (although these factors may used as specific suspect descriptions).

Category	Description
Observation/Surveillance	Demonstrating unusual interest in facilities, buildings, or infrastructure beyond mere casual or professional (e.g. engineers) interest such that a reasonable person would consider the activity suspicious. Examples include observation through binoculars, taking notes, attempting to measure distances, etc.
Materials Acquisition/Storage	Acquisition and/or storage of unusual quantities of materials such as cell phones, pagers, fuel, chemicals, toxic materials, and timers, such that a reasonable person would suspect possible criminal activity.
Acquisition of Expertise	Attempts to obtain or conduct training in security concepts; military weapons or tactics; or other unusual capabilities that would arouse suspicion in a reasonable person.
Weapons Discovery	Discovery of unusual amounts of weapons or explosives that would arouse suspicion in a reasonable person.
Sector-Specific Incident	Actions associated with a characteristic of unique concern to specific sectors (such as the public health sector), with regard to their personnel, facilities, systems or functions.

PART C – ISE-SAR INFORMATION FLOW DESCRIPTION

Step	Activity	Process	Notes
1	Observation	The information flow begins when a person observes behavior or activities that would appear suspicious to a reasonable person. Such activities could include, but are not limited to, expressed or implied threats, probing of security responses, site breach or physical intrusion, cyber attacks, indications of unusual public health sector activity, unauthorized attempts to obtain precursor chemical/agents or toxic materials, or other usual behavior or sector-specific incidents.[12]	The observer may be a private citizen, a government official, or a law enforcement officer.

[12] Suspicious activity reporting (SAR) is official documentation of observed behavior that may be reasonably indicative of intelligence gathering and/or pre-operational planning related to terrorism or other criminal activity. ISE-SARs are a subset of all SARs that have been determined by an appropriate authority to have a potential nexus to terrorism nexus (i.e., to be reasonably indicative of criminal activity associated with terrorism).

Step	Activity	Process	Notes
2	Initial Response and Investigation	An official of a Federal, State, local, or tribal agency with jurisdiction responds to the reported observation.[13] This official gathers additional facts through personal observations, interviews, and other investigative activities. This may, at the discretion of the official, require further observation or engaging the subject in conversation. Additional information acquired from such limited investigative activity could then be used to determine whether to dismiss the activity as innocent or escalate to the next step of the process. In the context of priority information requirements, as provided by State and major urban area fusion centers, the officer/agent may use a number of information systems to continue the investigation. These systems provide the officer/agent with a more complete picture of the activity being investigated. Some examples of such systems and the information they may provide include: Department of Motor Vehicles provides drivers license and vehicle registration information; National Crime Information Center provides wants and warrants information, criminal history information and access to the Terrorist Screening Center and the terrorist watch list, Violent Gang/Terrorism Organization File (VGTOF), and Regional Information Sharing System (RISS); Other Federal, State, local, and tribal systems can provide criminal checks within the immediate and surrounding jurisdictions. When the initial investigation is complete, the official documents the event. The report becomes the initial record for the law enforcement or Federal agency's records management system (RMS).	The event may be documented using a variety of reporting mechanisms and processes, including but not limited to, reports of investigation, event histories, field interviews (FI), citations, incident reports, and arrest reports. The record may be hard and/or soft copy and does not yet constitute an ISE-SAR.

[13] If a suspicious activity has a direct connection to terrorist activity the flow moves along an operational path. Depending upon urgency, the information could move immediately into law enforcement operations and lead to action against the identified terrorist activity. In this case, the suspicious activity would travel from the initial law enforcement contact directly to the law enforcement agency with enforcement responsibility.

Step	Activity	Process	Notes
3	Local/Regional Processing	The agency processes and stores the information in the RMS following agency policies and procedures. The flow will vary depending on whether the reporting organization is a State or local agency or a field element of a Federal agency. State, local, and tribal: Based on specific criteria or the nature of the activity observed, the State, local, and tribal law enforcement components forward the information to the State or major urban area fusion center for further analysis. Federal: Federal field components collecting suspicious activity would forward their reports to the appropriate resident, district, or division office. This information would be reported to field intelligence groups or headquarters elements through processes that vary from agency to agency. In addition to providing the information to its headquarters, the Federal field component would provide an information copy to the State or major urban area fusion center in its geographic region. This information contributes to the assessment of all suspicious activity in the State or major urban area fusion center's area of responsibility.	The State or major urban area fusion center should have access to all suspicious activity reporting in its geographic region whether collected by State, local, or tribal entities, or Federal field components.
4	Creation of an ISE-SAR	The determination of an ISE-SAR is a two-part process. First, at the State or major urban area fusion center or Federal agency, an analyst or law enforcement officer reviews the newly reported information against ISE-SAR behavior criteria. Second, based on available knowledge and information, the analyst or law enforcement officer determines whether the information meeting the criteria has a potential nexus to terrorism. Once this determination is made, the information becomes an "ISE-SAR" and is formatted in accordance with ISE-FS-200 (*ISE-SAR Functional Standard*). The ISE-SAR would then be shared with appropriate law enforcement and homeland security personnel in the State or major urban area fusion center's area of responsibility.	Some of this information may be used to develop criminal intelligence information or intelligence products which identifies trends and other terrorism related information and is derived from Federal agencies such as NCTC, DHS, and the FBI. For State, local, and tribal law enforcement, the ISE-SAR information may or may not meet the reasonable suspicion standard for criminal intelligence information. If it does, the information may also be submitted to a criminal intelligence information database and handled in accordance with 28 CFR Part 23.

Step	Activity	Process	Notes
5	ISE-SAR Sharing and Dissemination	In a State or major urban area fusion center, the ISE-SAR is shared with the appropriate FBI field components and the DHS representative and placed in the State or major urban area fusion center's ISE Shared Space or otherwise made available to members of the ISE. The FBI field component enters the ISE-SAR information into the FBI system and sends the information to FBI Headquarters. The DHS representative enters the ISE-SAR information into the DHS system and sends the information to DHS, Office of Intelligence Analysis.	
6	Federal Headquarters (HQ) Processing	At the Federal headquarters level, ISE-SAR information is combined with information from other State or major urban area fusion centers and Federal field components and incorporated into an agency-specific national threat assessment that is shared with ISE members. The ISE-SAR information may be provided to NCTC in the form of an agency-specific strategic threat assessment (e.g., strategic intelligence product).	
7	NCTC Analysis	When product(s) containing the ISE-SAR information are made available to NCTC, they are processed, collated, and analyzed with terrorism information from across the five communities—intelligence, defense, law enforcement, homeland security, and foreign affairs—and open sources. NCTC has the primary responsibility within the Federal government for analysis of terrorism information. NCTC produces federally coordinated analytic products that are shared through NCTC Online, the NCTC secure web site. The Interagency Threat Assessment and Coordinating Group (ITACG), housed at NCTC, facilitates the production of coordinated terrorism-related products that are focused on issues and needs of State, local, and tribal entities and when appropriate private sector entities. ITACG is the mechanism that facilitates the sharing of counterterrorism information with State, local, and tribal entities.	

Step	Activity	Process	Notes
8	NCTC Alerts, Warnings, Notifications	NCTC products[14], informed by the ITACG as appropriate, are shared with all appropriate Federal departments and agencies and with State, local, and tribal entities through the State or major urban area fusion centers. The sharing with State, local, and tribal entities and private sector occurs through the Federal departments or agencies that have been assigned the responsibility and have connectivity with the State or major urban area fusion centers. Some State or major urban area fusion centers, with secure connectivity and an NCTC Online account, can access NCTC products directly. State or major urban area fusion centers will use NCTC and ITACG informed products to help develop geographic-specific risk assessments (GSRA) to facilitate regional counterterrorism efforts. The GSRA are shared with State, local, and tribal entities and the private sector as appropriate. The recipient of the GSRA may use the GSRA to develop information gathering priorities or requirements.	NCTC products form the foundation of informational needs and guide collection of additional information. NCTC products should be responsive to informational needs of State, local, and tribal entities.
9	Focused Collection	The information has come full circle and the process begins again, informed by an NCTC or other Federal organization's product and the identified information needs of State, local and tribal entities and Federal field components.	

[14] NCTC product include: Alerts, warnings, and notifications—identifying time sensitive or strategic threats; Situational awareness reports; and Strategic and foundational assessments of terrorist risks and threats to the United States and related intelligence information.

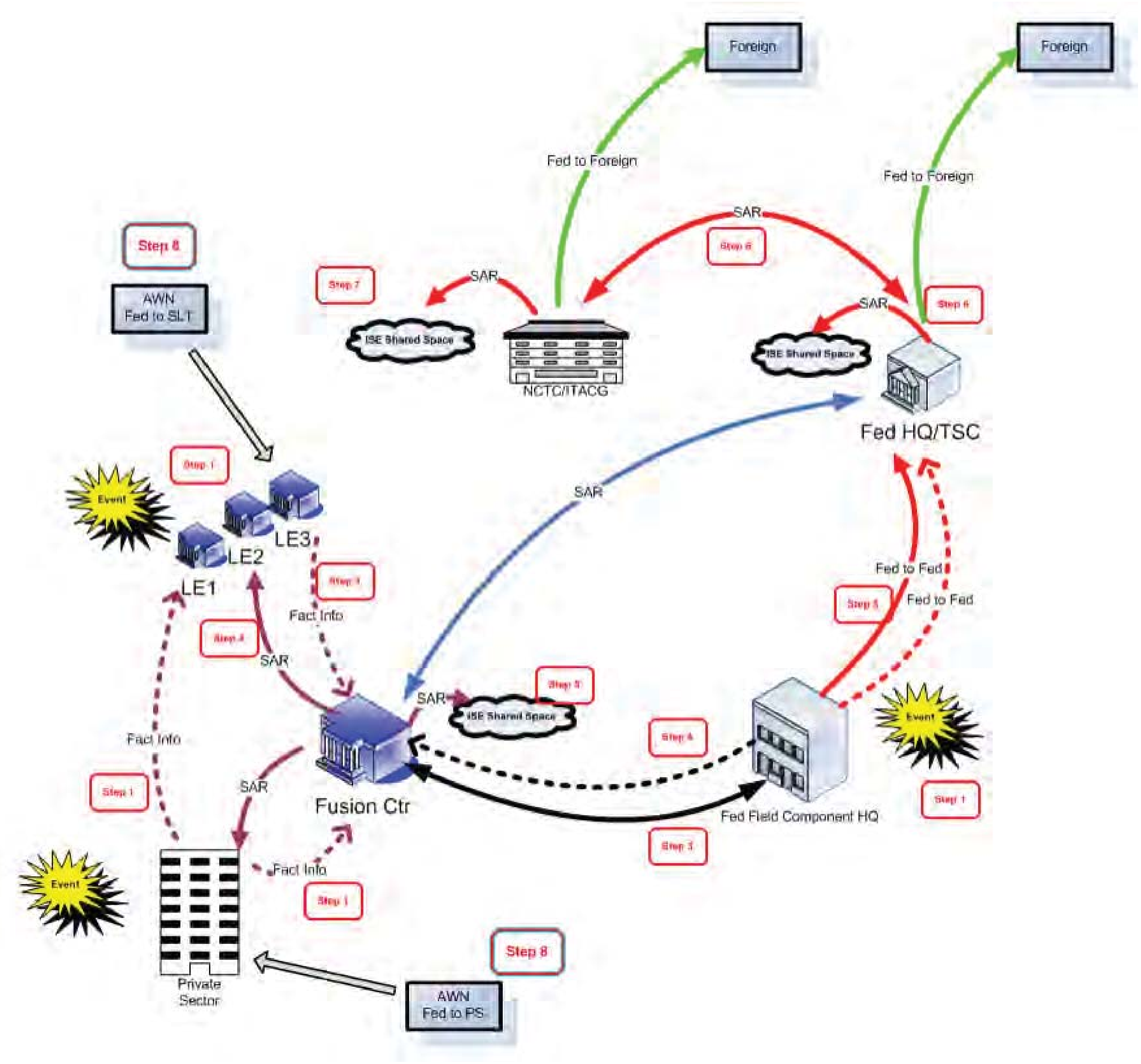

Foreign
Foreign
Fed to Foreign
Fed to Foreign
SAR
SAR
SAR
Step 8
AWN
Fed to SLT
ISE Shared Space
NCTC/ITACG
ISE Shared Space
Fed HQ/TSC
Event
LE3
LE2
LE1
SAR
Fact Info
SAR
Fed to Fed
Fed to Fed
SAR
ISE Shared Space
Fact Info
Event
SAR
Fusion Ctr
Fed Field Component HQ
Event
Fact Info
Private
Sector
Step 8
AWN
Fed to PS

Figure 3 – SAR Information Flow Diagram

Exhibit E

Privacy Impact Assessment for the eGuardian Threat Tracking System

Responsible Officials

Counterterrorism Division

Program Manager

[redacted]

Threat Monitoring Unit (TMU)

[redacted]

System Developer

[redacted]

Foreign Terrorist Tracking Task Force (FTTTF)

[redacted]

Reviewing Officials

[redacted]

Chief Privacy and Civil Liberties Officer
Federal Bureau of Investigation

[redacted]

Chief Information Officer
Department of Justice

Approving Official

[redacted]

Acting Chief Privacy Officer and Civil Liberties Officer
Department of Justice

b6
b7C

November 25, 2008

ACLUEG000047

FINAL

INTRODUCTION

Overview

The National Threat Center Section (NTCS) in the FBI's Counterterrorism Division is the focal point for all threat information, preliminary analysis, and assignment for immediate action of all emerging International Terrorism and Domestic Terrorism threats incoming to the FBI. Within NTCS, the Threat Monitoring Unit (TMU) has the primary responsibility for supporting the FBI's role in defending the United States against terrorism threats. Through coordination with FBI Field Offices, Legal Attaches, and other government agencies, TMU collects, assesses, disseminates, and memorializes all threat information collected or received by the FBI. A companion unit to TMU, the Threat Review Unit (TRU), analyzes the threat information that is collected in order to identify trends and prepares informational products that can be shared.

To help it accomplish its work, in 2003, TMU developed the Guardian Program.[1] Guardian is an information technology system maintained at the Secret level that allows TMU to collect suspicious activity reports (SARs) made to the FBI and review the SARs in an organized way to determine which ones warrant additional investigative follow-up. Guardian's primary purpose is not to manage cases, but to facilitate the reporting, tracking, and management of threats to determine within a short time span (30 days or less) whether a particular matter should be closed or referred for an investigation. Guardian also facilitates the TRU's work in performing its analytical functions because the reports are available for pattern and trend analysis.

Because of the mandate, expressed in the Intelligence Reform and Terrorism Prevention Act as well as in other statutes and Executive Orders and in the National Strategy for Combating Terrorism, to share terrorism information with other federal, and state, local and tribal (SLT) law enforcement partners, the FBI now proposes to create an unclassified version of its Guardian Program – called eGuardian – that will provide participating partners with access to a reporting system to be hosted on a secure but unclassified Internet network that will be accessed through Law Enforcement Online (LEO). The SARs that are contributed to eGuardian, after initial approval, will be accessible to specially-vetted representatives of other federal law enforcement partners and SLT law enforcement partners. These SARs should help facilitate situational awareness with respect to potential terrorism threats. Sharing these reports should eliminate the jurisdictional and bureaucratic impediments that otherwise delay communication of this important information that is necessary to enhance our national security posture.

Information Sources

The threat information to be contributed to eGuardian may come from three sources: (1) unclassified information from the FBI's Guardian system; (2) reports from other federal agencies with law enforcement functions, including components of the

[1] The Guardian Program was the subject of a Privacy Impact Assessment dated April 13, 2005.

ACLUEG000048

Department of Homeland Security[2] and law enforcement investigative services within the Department of Defense;[3] and (3) SARs contributed by SLT law enforcement.

Unclassified information from the Guardian system that appears to have a potential nexus to terrorism will be passed down to eGuardian, where it will be available for viewing by the participants of eGuardian, including those members of SLT law enforcement and representatives of other federal law enforcement agencies that have been given permission to access the eGuardian system.

For the information coming from other federal agencies with law enforcement functions, including FBI unclassified reporting passed through Guardian Express, TMU will conduct the initial screening of federal suspicious activity reports, other than reports by law enforcement investigative services within DoD. Suspicious activity reports from law enforcement investigative services within DoD will be analyzed in a DoD fusion center-like organization for a further determination whether the information warrants contribution to eGuardian (labeled as the Shared Data Repository (SDR) on Diagram 1.a) and then on into Guardian.

Suspicious Activity Reports from SLT partners will be submitted to the appropriate State or Local Fusion Center for a similar analysis there. If the Fusion Center accepts a report as demonstrating a potential nexus to terrorism, it will be submitted to the SDR and then on into Guardian for the FBI to analyze further to determine if investigative action at the Federal level is warranted. Additionally, once the report is in the SDR, it will be available for viewing by the participants of eGuardian.

From each of these sources, those reports that appear to have a potential nexus to terrorism will be added to the Guardian system for further analysis. Incidents and threats that are found to warrant investigation will be assigned, via Guardian, to a member of one of the FBI's Joint Terrorism Task Forces (JTTFs). Nationwide, all 56 FBI field divisions maintain at least one JTTF. The JTTFs are comprised of SLT law enforcement officers who are deputized as federal agents, as well as law enforcement agents from other federal agencies, including the Department of Homeland Security and the Department of Defense. The JTTFs have the primary responsibility for investigating terrorist threats, events, and suspicious activities with a potential nexus to terrorism.

The eGuardian system will be used to record, review, sort, and prioritize these counterterrorism threats and suspicious activity incidents and present the information to law enforcement partners who will access the eGuardian SDR through a Special Interest Group accessed through LEO. Law enforcement agencies that have contributed information will have read and write access to their reports in the SDR in order to update them as necessary. Other law enforcement partners will have read-only access to the

[2] These include the Federal Air Marshals Service, Immigration and Customs Enforcement, Customs and Border Protection, and the United States Coast Guard.

[3] These include the Army Criminal Investigation Command (CID), the Naval Criminal Investigative Service, and the Air Force Office of Special Investigations. Other DOD components with force protection law enforcement arrest authority may also participate in eGuardian, such as the Pentagon Force Protection Agency.

SDR to ensure appropriate dissemination of these counterterrorism threats and suspicious activity incidents.

Review Process

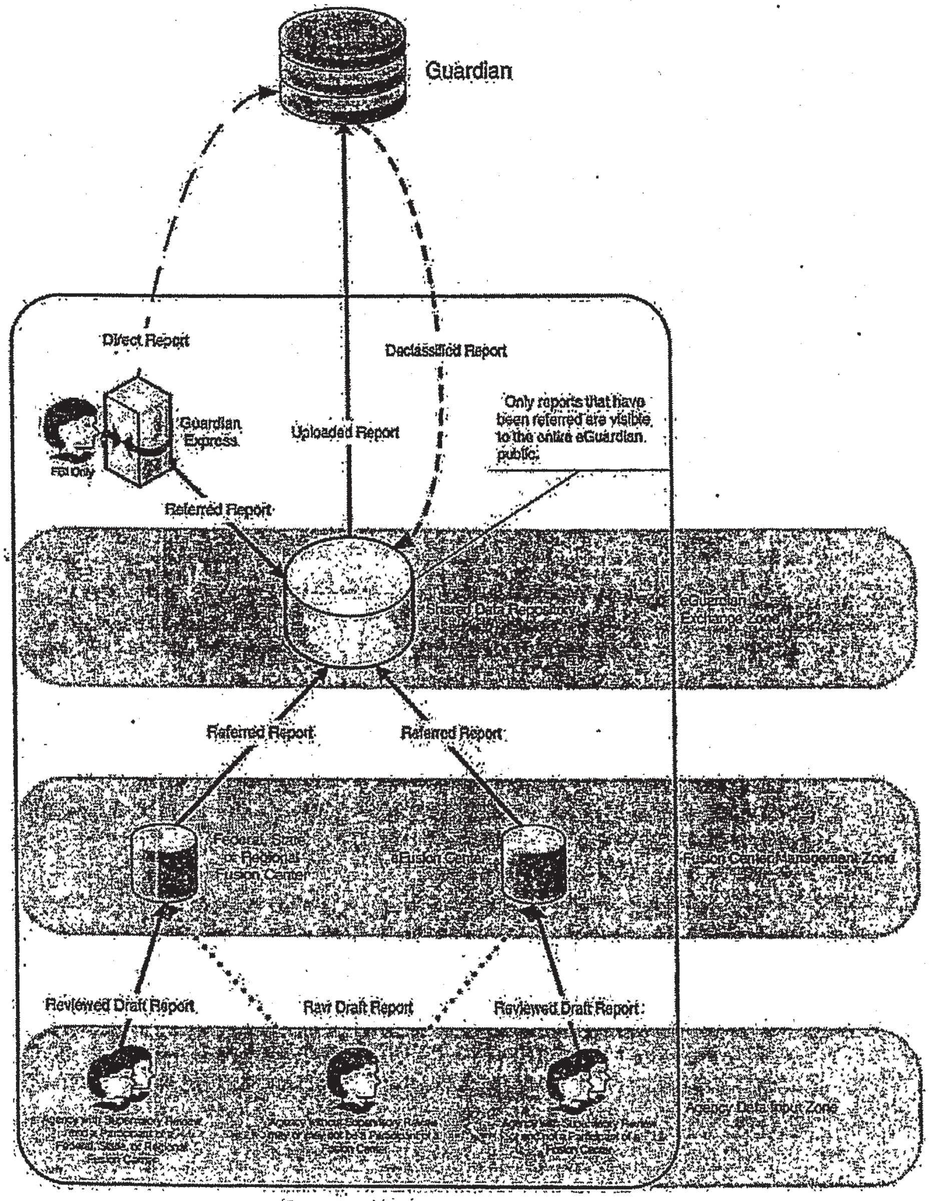
Throughout the initial threat reporting process, regardless of where the report originates, if a determination is made of "no nexus to terrorism," the information will not be added to the eGuardian SDR. Additionally, at the Fusion Center level, the information will be deleted. If a clear determination is made of "a nexus to terrorism," the information will be passed along to the eGuardian SDR for further dissemination and then on to Guardian for analysis. If no determination can be made regarding "a nexus to terrorism," but neither can the nexus be discounted, the information will be added to the eGuardian SDR for pattern and trend analysis.

In keeping with the retention period currently in effect for state criminal intelligence systems under 28 C.F.R. Part 23, suspicious activity reports in this third category (reports for which a determination cannot be made whether or not a nexus to terrorism exists) will be retained for a period of five years and will be used for analytical purposes and/or to demonstrate trends. eGuardian considers all reports submitted to the system to be the property of the submitting agency; therefore, should a submitting agency desire that a report be removed from the system prior to the five-year mark, the report will be removed. Otherwise these reports also can be available for trend and other analyses.

User Access/Security

The eGuardian system will ensure consistency of process and of handling protocols by using a uniform user agreement for each agency or law enforcement entity that connects to eGuardian through LEO. By signing the user agreement, the parties will agree to the Fusion Center or TMU policies, which reflect the conditions of use and privacy and security requirements of eGuardian. All users will be required to assent to these rules of behavior each time they log on to the system. Additionally, all users will be required to complete robust system training that will incorporate eGuardian policies and procedures concerning privacy and civil liberties. Audit controls will be employed to ensure that the use of eGuardian is consistent with its intended purpose.

The following diagram (Diagram 1a) provides an overview of the eGuardian system described in this Privacy Impact Assessment. Data is input at an initial level but reviewed at a Fusion Center or similar entity before being passed to eGuardian if the information appears to be linked to terrorism. The "Agency Data Input Zone" represents law enforcement contributors of suspicious activity reports with a potential nexus to terrorism. The Fusion Center Management Zone represents the vetting that must occur before these reports are shared with eGuardian participants. The eGuardian Exchange Zone is where this information sharing will actually occur, once a determination has been made that the report has a potential nexus to terrorism. The FBI's role is to serve as both a contributor of information from its Guardian system and a recipient of eGuardian reports that warrant additional investigation at the Federal level.


Guardian
Direct Report
Declassified Report
Guardian Express
FBI Only
Uploaded Report
Only reports that have been referred are visible to the entire eGuardian public.
Referred Report
Shared Data Repository
eGuardian
Exchange Zone
Referred Report
Referred Report
Federal, State or Regional Fusion Center
eFusion Center
Fusion Center Management Zone
Reviewed Draft Report
Ravi Draft Report
Reviewed Draft Report
Agency Data Input Zone

e-Guardian System
Internal Data Flows

Diagram 1a

ACLUEG000051

Section 1.0
The System and the Information Collected and Stored within the System

1.1 What information is to be collected?

eGuardian will collect terrorism threat information and/or suspicious activity information having a potential nexus to terrorism. "Suspicious activity" is defined as observed behavior that may be indicative of intelligence gathering or pre-operational planning related to terrorism, criminal or other illicit intention. This definition is consistent with the definition utilized by the Program Manager/Information Sharing Environment (PM/ISE). Suspicious activities may include surveillance, cyber attacks, probing of security and photography of key infrastructure facilities. Personally identifiable information (PII) to be collected will include all available identifiers regarding the subject of a report or incident, such as name, date and place of birth, unique identifying numbers, physical description, and similar attributes.

1.2 From whom is the information collected?

Suspicious activity reports and threats that have a potential nexus to terrorism may be reported to law enforcement from private citizens or may come directly from law enforcement personnel who observe or investigate activities.

1.3 Privacy Impact Analysis: Given the amount and type of data collected, discuss the privacy risks identified and how they were mitigated.

FBI suspicious activity reports that are entered into eGuardian at the federal level will have been analyzed initially by TMU to determine whether sufficient facts exist to warrant placement of the information into the system. Suspicious activity reports from SLT law enforcement and other federal agencies will be required to pass through a Fusion Center or similar analytical construct prior to being passed to eGuardian. In all cases of data ingest, trained analysts or law enforcement personnel will make the judgment that the information rises sufficiently to the level that a report should be added to eGuardian.

eGuardian users will be advised in an online tutorial that frequent checking of the database for updates will be necessary, at intervals no less than 30 days, and will be encouraged to ensure that information they have entered initially is supplemented whenever new facts are uncovered. In the work flow that is created for eGuardian, contributors will be able to add notes that help clarify the contributed information.

eGuardian has developed a set of guidelines for the types of information that *cannot* be entered into the system by any participating entity, including the FBI. For example, no entry may be made into eGuardian based solely on the ethnicity, race or religion of an individual or solely on the exercise of rights guaranteed by the First Amendment or the lawful exercise of any other rights secured by the Constitution or the laws of the United States. These restrictions will be prominently displayed when an individual accesses eGuardian and he or she will have to affirmatively indicate agreement to abide by these rules before being permitted to proceed to view reports.

In addition, the following specific categories of information will not be permitted to be entered into eGuardian: classified information; information that divulges sensitive methods and techniques; FISA-derived information; grand jury information; federal taxpayer information; sealed indictments; sealed court proceedings; confidential human source and witness information; Title III subject and intercept information; and other information that is subject to legal restriction. The eGuardian Program Manager will have personnel assigned to monitor the system to ensure that these categories of information are not included in eGuardian reports.

All information will be subject to threshold screening by the submitting law enforcement officer before being placed in the system and then will be submitted to a Fusion Center, to TMU or to the DOD fusion center-like organization [hereinafter collectively referred to as a "responsible entity"] within the Fusion Center Management Zone (see Diagram 1a) for a decision regarding adding the report to eGuardian. This screening will ensure that trained law enforcement personnel and/or analysts make the initial decision that a report warrants further review. Furthermore, the eGuardian workflow architecture is designed to restrict the ability to view submitted reports to the reporter, the reporter's supervisor, and the approving responsible entity. Incidents submitted to eGuardian will not be viewable to the eGuardian users outside this workflow until the report is approved at the responsible entity level.

Section 2.0
The Purpose of the System and the Information Collected and Stored within the System.

2.1 Why is the information being collected?

The National Strategy for Combating Terrorism recognizes that the war on terror requires greater flexibility and resilience to confront threats facing our nation from a transnational terrorism movement designed to destroy our way of life. The collection of information in eGuardian is consistent with this national strategy and also with the emphasis placed by the President and the Congress on sharing terrorism information with our law enforcement partners. It also recognizes that the police officer on the street is often in the best position to observe suspicious behavior that may have national security implications. eGuardian and Guardian provide a dynamic tool to accomplish this sharing to increase awareness and foster review of threats and suspicious activities in a timely manner so that they can be mitigated appropriately. It is also very important to note that eGuardian is at its very essence, simply a platform to standardize the disparate SAR systems currently utilized by agencies to collect information, which will enhance communication among law enforcement entities as well as situational awareness.

2.2 What specific legal authorities, arrangements, and /or agreements authorize the collection of information?

The FBI's general investigative authority in 28 U.S.C. 533 and its general authority to collect records in 28 U.S.C. 534 provide the statutory basis for the activities ascribed to eGuardian. The FBI is also assigned the lead role in investigating terrorism and in the collection of terrorism threat information within the United States by 28 C.F.R. § 0.85 and Annex II to National Security Presidential Directive 46. In addition, the Intelligence Reform and Terrorism Prevention Act requires the President to establish an information sharing environment for sharing terrorism information in a manner that is consistent with national security and applicable legal standards pertaining to privacy and civil liberties. Further, the President's National Strategy for Information Sharing supports the eGuardian initiative; it identifies suspicious activity reporting as one of the key information exchanges between the Federal Government and State and local partners.

2.3 Privacy Impact Analysis: Given the amount and type of information collected, as well as the purpose, discuss what privacy risks were identified and how they were mitigated.

The most significant privacy risk is that information which first appears to be suspicious will turn out, upon further vetting, to be innocuous, resulting in the over collection of data. A related significant risk is that dissemination of personal information will be overly broad and will include agency officials who have no need to know the information. Both risks are mitigated in several ways.

First, a standard definition of what constitutes a suspicious activity will be used by all participating agencies. As mentioned previously, the suspicious activity definition will be the definition currently developed by the PM/ISE. The PM/ISE suspicious activity definition will be augmented by describing the kinds of information that cannot be entered into the system. The definition with these qualifiers will be incorporated into the User Agreement that appears on the LEO eGuardian Special Interest Group page where eGuardian incidents will be placed and individuals accessing the system will have to confirm that they have read and understand the Agreement and agree to be bound by the constraints articulated therein.

Second, eGuardian is intended to function as an alert, recording and reporting system and not as a long-term data repository. As a result, decisions about SARs will be made promptly so that the data can move quickly through the system. All SLT and federal law enforcement agencies with missions that pertain to homeland security will be encouraged to enter terrorism-related threats and suspicious activity incidents into eGuardian for an appraisal by the appropriate Fusion Center, the FBI's TMU or the DOD equivalent.

In general, Fusion Centers are becoming the focal points for information sharing and will function as an additional layer of review to confirm that the incident warrants treatment as suspicious or potentially connected to terrorism. With the proper training of personnel who perform system management and analytical functions (as discussed elsewhere in this assessment), the use of Fusion Centers as an intermediary should lead to an effective and standardized vetting process that moves reports quickly through the eGuardian system. There will be vigorous efforts to police eGuardian and eliminate irrelevant, erroneous or otherwise improper reporting. Suspicious activity, incidents and threats that are found to warrant investigation due to a likelihood of having a potential terrorism nexus will be assigned to a member of the FBI's Joint Terrorism Task Forces (JTTFs).

Within the eGuardian system, suspicious activity reports that appear to have a potential nexus to terrorism will be entered by the FBI or a law enforcement partner into the eGuardian system where a record will be created to summarize the nature of the incident for subsequent analytical assessment. The assessment is intended to take place within no more than 30 days and result in one of the following dispositions:

1. DRAFT – threat or report of suspicious activity is reported to the agency reporting space (see Diagram 1a for information flow from Agency Data Input Zone to Fusion Center Management Zone) eGuardian system by an authorized user;
2. REFERRED – a threat or report of suspicious activity has been referred to the SDR of eGuardian (see Diagram 1a for information flow from Fusion Center Management Zone to eGuardian Exchange Zone) and uploaded to Guardian for further assessment by a FBI/JTTF investigator; or
3. CLOSED – a threat or report of suspicious activity has been reviewed and found to have no nexus to terrorism.

The eGuardian system handles Draft reports in two ways depending on where in the eGuardian workflow the draft exists and how the agency has configured their agency eGuardian workflow. When an agency creates (enters) a suspicious activity report in the eGuardian system, the report is only visible to the eGuardian account holders from that agency. At this point the report is considered to be at agency-level control (see Diagram 1a, Agency Data Input Zone). The report cannot be seen by the Fusion Center responsible for the agency nor can it be seen by the FBI or any other law enforcement agency (LEO eGuardian Special Interest Group). This design enhances privacy protection by restricting access to PII to the agency that created the report. This design function also allows the agency complete control over information they enter into eGuardian.

At the Agency Data Input Zone, the agency reporter or the agency supervisor (if applicable) may elect to retain the information with the eGuardian system pursuant to their agency policy, but for no more than five years. The agency makes the determination whether to share the report by submitting it to their responsible Fusion Center or the TMU, if the agency does not participate in a Fusion Center. The agency may also decide to close the report. If the agency closes the report at the agency level, neither the Fusion Center nor the FBI nor any other agency will ever see the report. If the agency elects to submit the incident to the appropriate Fusion Center, the report continues to remain in draft status and becomes viewable only by the responsible Fusion Center and the FBI. The Draft report is not yet viewable to other law enforcement partners. At the Fusion Center Management Zone (see Diagram 1a), the draft report will be analyzed in an attempt to identify a potential nexus to terrorism.

As noted above, if the Draft report is determined to have no nexus to terrorism, the Draft report will be closed by the Fusion Center and will not be made available for viewing by any other law enforcement partner. Furthermore, closed Draft reports that are determined to have no nexus to terrorism will be deleted from the eGuardian system.

Draft reports in which a threat or report of suspicious activity is indeed found by the appropriate Fusion Center, including the FBI's TMU or DOD equivalent, to have a potential nexus to terrorism are passed to the eGuardian SDR in the eGuardian Exchange Zone and loaded into Guardian. The copy of the report retained in eGuardian will have its status changed from Draft to Referred. At this point the report will be viewable to other law enforcement partners that are members of the LEO eGuardian Special Interest Group. Also, as noted above, if a nexus to terrorism can neither be substantiated nor discounted, the Referred report is determined to be inconclusive, marked as such, and then referred to Guardian for further assessment by the JTTF. Again, at this point, the Referred report will be viewable to other law enforcement agencies with eGuardian accounts. The report will continue to remain in the eGuardian system for tracking and further analytic review. The information in these reports – where a nexus to terrorism is inconclusive or a nexus to terrorism has been substantiated – will be maintained for five years.

This illustrates that the eGuardian workflows heavily restrict information while in "Draft" stage. Reports are only accessible to the eGuardian user community after a potential terrorism nexus is identified or the report is found to be inconclusive in which case the report remains in eGuardian and is referred to Guardian for additional assessment and/or investigation. Likewise, inconclusive reports may later be closed and deleted if, after subsequent analytical evaluation or the passage of time, the report is found to be erroneous, irrelevant or later determined to have no nexus to terrorism.

In addition, in terms of access to the system, the eGuardian user community will consist of only those law enforcement partners who qualify for access to LEO and who are specifically granted access to the eGuardian SIG by TMU.

Other ways that the privacy risk presented by this system is mitigated is through the use of technology. eGuardian will have the ability to conduct data optimization which will identify and eliminate duplicate data objects. This will improve the quality of the data. The system will also be able to provide data segmentation so that disparate rules of SLT law enforcement and federal agencies for limiting collection and access can be implemented. In other words, different rules regarding retention and use that are required by state laws can be incorporated as attributes of the contributed data. Finally, as noted above, the retention period for eGuardian reports generally will be relatively short (5 years) in an effort to balance the need to retain information long enough to discern potential terrorism planning activities but short enough to protect the privacy of individuals whose information is maintained.

Section 3.0
Uses of the System and the Information

3.1 Describe all uses of the information.

eGuardian is first and foremost a reporting system that standardizes existing reporting. Reports will be placed into eGuardian to assist in assessing terrorism-related threats and suspicious activities. In addition, the information derived from the reports that are placed in eGuardian may show links, relationships, and matches among data elements, which will provide the opportunity for analysis and interpretation. The use of the tools in eGuardian will enable analysts, officers, detectives, agents, and other law enforcement investigators to develop leads and identify potential suspects more quickly. Once vetted by a responsible entity, this information will be shared with law enforcement at all levels in order to more effectively identify threats and threat patterns and take actions to mitigate such threats.

3.2 Does the system analyze data to assist users in identifying previously unknown areas of note, concern, or pattern? (Sometimes referred to as data mining.)

The eGuardian system will contain an analytical functionality to find potential links and patterns between terrorism suspects and suspicious events. Rather than facilitating the search for anomalies based on patterns, however, the point of the system is to collect reports about activities that may be linked to terrorism and then to refer the information for further investigation as necessary and to analyze it for potential linkages that can enhance the ability of the FBI and other law enforcement agencies to take preventative action. There is no capability to use eGuardian for pattern-based data mining as described in section 804 of the Implementing Recommendations of the 9/11 Commission Act of 2007. Should that capability be added and exploited for pattern-based data mining, this assessment will be updated and the activity will be reported to Congress as required by the Act.

3.3 How will the information collected from individuals or derived from the system, including the system itself, be checked for accuracy?

The data will be collected in accordance with procedures established by the respective agencies' policies for collecting data related to suspicious activities that may pertain to terrorism. The information will then be examined by trained investigators for accuracy and authenticity. The system itself will be able to identify duplicate data items and all records will be date and time-stamped. Information that is forwarded to Fusion Centers from SLT law enforcement partners will be subject to additional checks for accuracy and the integrated data available at the Fusion Centers will be utilized to help determine information that is accurate or that is suspect.

3.4 What is the retention period for the data in the system? Has the applicable retention scheduled been approved by the National Archives and Records Administration (NARA)?

e-Guardian has coordinated records retention policies with the FBI's Records Management Division. A determination has been made that information contributed by SLT and other federal agency partners remains under the control of those agencies. The reports that are maintained in the eGuardian SDR are also uploaded to the FBI's Guardian system. The retention schedule for Guardian records will therefore be applied to this information, which will be retained in that system.

As noted earlier, information entered into eGuardian will be characterized in one of three ways: initially, the reported incident will remain in "DRAFT" status until such time as the incident is approved, normally by the responsible entity. While in draft form, the incident is only viewable by the originating agency reporter, and the reporter's supervisor if applicable. If the agency reporter's supervisor decides to share the report outside the originating agency, the supervisor submits the report to the responsible Fusion Center. At this point, the report is only viewable by the reporter, the reporter's supervisor(s), the responsible Fusion Center Administrators and TMU (eFusion Center) personnel. When the incident appears to have a potential nexus to terrorism, upon approval the categorization will change to "REFERRED." Referred indicates the incident has been electronically forwarded, or referred, to the FBI JTTF/Guardian squad for further investigative assessment. If a nexus to terrorism can neither be substantiated nor discounted, the incident remains as "REFERRED," and it will stay in the system for tracking and analytic review. If no nexus to terrorism is established for a particular incident, it will be deleted from the eGuardian system.[4]

3.5 Privacy Impact Analysis: Describe any types of controls that may be in place to ensure that information is handled in accordance with the above described uses.

Access to eGuardian will be available through a secure interface to Law Enforcement Online (LEO). LEO, which is a sensitive but unclassified and for authorized use only secure web-based network containing only authorized membership, will provide authentication services for eGuardian users. Each individual LEO user is issued and required to use a login and password that is unique to that user. Passwords must be changed every 90 days. eGuardian will be accessed through a Special Interest Group (SIG) on LEO. Membership in the SIG is by application only and will be drawn only from agencies that have an originating agency identifier (ORI) and thus are recognized law enforcement entities. Membership must also be approved by TMU. In the event an agency with an operational need to share/receive information does not have an ORI, one will be created for that agency by the eGuardian developers/programmers provided appropriate criteria are met. The use of an ORI designation will help to ensure that only those law enforcement personnel who have been cleared for access actually have it. Furthermore, members of the SIG will have to agree to a User Agreement each time they log in to eGuardian that dictates how information in the system is to be ingested, maintained and disseminated. The User Agreement will counsel that recorded information should be accurate to the extent possible, timely and relevant to a suspicious activity with a potential nexus to terrorism. Users will be cautioned not to enter information that describes First Amendment protected activities or personal information based solely on ethnicity, race or religion. SIG users' activities while online will be tracked and available for audit so that these rules can be enforced.

---

[4] Information that suggests possible criminal activity may be referred to the appropriate division in the FBI. See section 4.2 below.

Other safeguards to ensure compliance with proper use rules include the limited exposure and non-retention for incidents that do not clear Fusion Center vetting; the retention and deletion controls enforced by the eGuardian system administrator; and the ability to audit and trace user identification if improper use is discovered.

Section 4
Internal Sharing and Disclosure of Information within the System.

4.1 With which internal components of the Department is the information shared?

Other DOJ components, including but not limited to the criminal components of the Department of Justice will be provided access to eGuardian if they have an operational need to know the potential terrorism information that the system contains. To the extent that information is received by TMU that pertains to potential criminal offenses with no apparent nexus to terrorism, and thus it is not appropriate for entry into eGuardian, it may be shared or forwarded to the appropriate division within the FBI or within the Department of Justice for further handling. While the information will not reside in eGuardian, referral of information about potential criminal offenses is consistent with current FBI.

4.2 For each recipient component or office, what information is shared and for what purpose?

Information with a potential nexus to terrorism will be shared with other DOJ components that have an operational need to receive the information.

Some information that is entered into eGuardian may reflect potential criminal conduct, but not conduct that amounts to terrorism. That information will be forwarded to the FBI's Criminal Investigative Division or other responsible law enforcement agency for appropriate disposition. This is not unlike the current situation in which members of the public or law enforcement personnel report incidents that are suspicious or otherwise to an FBI Field Office and the Field Office takes action to mitigate the information – either by forwarding it to the appropriate office for disposition, using it as the basis for additional investigative activity, or closing it as reflecting no violation of law.

4.3 How is the information transmitted or disclosed?

Information will be made available electronically through the eGuardian network or through secure electronic media.

4.4 Privacy Impact Analysis: Given the internal sharing, discuss what privacy risks were identified and how they were mitigated.

Sharing personally identifiable information carries with it a risk of improper access and/or improper use. The Privacy Act governs the dissemination of information internally within an agency; it is appropriate when there is a need to know. Because other DOJ law enforcement components are expected to be the prime recipients of any data that is shared internally, the internal sharing that is contemplated will meet the Privacy Act requirement. Cookies, which are pieces of text stored on an agency user's computer hard disk, will be used, imbedded in the program, to track access to specific information. Also, only after the incident is approved and REFERRED to Guardian by the Fusion Center is it visible to anyone beyond the original user, the user's immediate supervisor(s), the Fusion Center, and TMU. There is also a risk of data breach from the SIG, but the security features of LEO, coupled with the ability to audit system users, should help mitigate this risk.

Section 5
External Sharing and Disclosure

5.1 With which external (non-DOJ) recipient(s) is the information shared?

Consistent with the National Strategy for Information Sharing, vetted eGuardian information is intended to be shared with other Federal, State, local and tribal law enforcement agencies, including task force members and analytical support personnel.

5.2 What information is shared and for what purpose?

Suspicious activity or threat information having a potential nexus to terrorism will be shared with the goal of creating an efficient, near real-time mechanism for law enforcement at the State, local, tribal and federal level to share and report terrorist threat data and suspicious activity and to discern any otherwise unknown relationships among reported incidents.

5.3 How is the information transmitted or disclosed?

Information is made accessible either through eGuardian, which will be in a SIG on LEO or hard copy information may be printed and disseminated. Section 3.5 describes how information will be accessed in greater detail. The potential also exists for wireless access to the SIG. User agreements will require that information obtained through eGuardian shall not be re-disseminated without approval of a responsible entity or the originating entity.

5.4 Are there any agreements concerning the security and privacy of the data once it is shared?

By logging onto the SIG, an eGuardian user will be provided a set of behavioral rules, in addition to the standard login disclaimer about the sensitivity of the information, which will describe expectations for use of the information (see attachment 1). In addition, although law enforcement personnel with access to eGuardian are trained officials and understand the rules concerning dissemination of information, additional web-based training of users on the security and privacy requirements of the system as well as system functionality will be provided by LEO. A caveat identifying eGuardian information as Sensitive but Unclassified and For Official Use Only will be included in any dissemination. It is anticipated that these labels will be replaced by a uniform designation as a matter of federal policy; when that policy is fully implemented, the caveat in eGuardian will be amended as required.

5.5 What type of training is required for users from agencies outside DOJ prior to receiving access to the information?

As noted in the previous answer, Web-based training for all users will be required as part of the eGuardian system.

5.6 Are there any provisions in place for auditing the recipients' use of the information?

All users will have to agree to the User Agreement before being granted access, and caveats about use of eGuardian information will be part of the Agreement. Additionally, the required training for all eGuardian users will cover subsequent use of the information. eGuardian will have the capability to determine who has accessed the system and what data they have created or modified and; thereby, will be able to identify the responsible users if incidents of inappropriate use or disclosure are reported. In addition, periodic audit log reviews will be used to discover access patterns as well as indications of inappropriate access, which will lead to firm controls over users, and can also generate leads to inquire into their use of the data.

5.7 Privacy Impact Analysis: Given the external sharing, what privacy risks were identified and describe how they were mitigated.

7C

Access to eGuardian via LEO is controlled by the LEO network itself. Users obtain access to LEO by applying for and receiving a LEO network login and password, which is only granted to authorized law enforcement agencies. Passwords must be changed every 90 days and any information that is transmitted will meet current security standards. eGuardian will be accessible through a Special Interest Group (SIG). Membership to the eGuardian SIG is by application only. Account holders will be vetted by the applicant's agency. The agency must have an ORI signifying that it is a recognized law enforcement entity. Finally, agencies must apply for membership in the SIG and be approved by TMU. In the event an agency with an operational necessity to share/receive information does not have an ORI, one will be created for that agency by the eGuardian developers/programmers. This security control should help mitigate the privacy risk that arises from inappropriate access to the data. In further mitigation, audit logs of search transactions will be reviewed every 180 days to check for anomalous activity. TMU will have the ability to delete user accounts at the individual or agency level. Finally, training on using eGuardian will be provided and this training will help ensure that users fully understand the User Agreement concerning dissemination of information. Given the anticipated large number of external users, the risk of misuse of the information or unauthorized access and dissemination of the information by even a trained user always exists. That risk is mitigated significantly by both the restrictions on access to--and dissemination of--unvetted information, as described above, as well as by the audit features noted in Section 5.6 above.

Another privacy risk is that the sum of the data entered into eGuardian may be greater than its component parts, with the result that new and different information about incidents and people alleged to be suspicious becomes apparent. This is, in significant part, the purpose of the system, but it also creates a privacy risk, as well as a risk of public misperception and possible misunderstanding. The privacy risk is that seemingly isolated incidents or observations may lead to more discovery of personal information about individuals in an effort to develop relationships (i.e., "connect the dots") between these and other incidents and observations. This risk is mitigated in part by the inherent nature of the process; i.e., in the end only meaningful relationships that affect national security will be developed and acted upon. The incidents or observations containing personal information that remain isolated or the relationships among incidents that do not develop investigative value will not lead to further action and will be retained in eGuardian for the limited time indicated above. These on-going vetting and analytical processes should minimize the risk of unwarranted and inappropriate dissemination of irrelevant personal information.

Section 6.0
Notice

6.1 Was any form of notice provided to the individual prior to collection of information? (If yes, please provide a copy of the notice as an appendix. A notice may include a posted privacy policy, a Privacy Act notice on forms, or a system of records notice published in the Federal Register.) If notice was not provided, why not?

General notice concerning the FBI's collection, use and maintenance of law enforcement and intelligence information is provided through the System of Records Notice for the Central Records System (63 Fed. Reg. 8671). As noted above, that notice describes the fact that the FBI maintains computerized investigative information extracted from its own files or those of other governmental sources. Because the collection of eGuardian information may be done in connection with law enforcement activities, no individual notice will be given.

6.2 Do individuals have an opportunity and/or right to decline to provide information?

eGuardian suspicious activity reports, in many cases, will originate from observations made by law enforcement officers and from information received from the general public. In those situations, no opportunity or right to decline information is provided. The reports that are submitted are nevertheless vetted by trained law enforcement personnel and funneled through a second review at a Fusion Center or comparable entity before being added to the system.

6.3 Do individuals have an opportunity to consent to particular uses of the information, and if so, what is the procedure by which an individual would provide such consent?

Because of the nature of the records at issue, the opportunity to consent to particular uses of the information is not provided.

6.4 Privacy Impact Analysis: Given the notice provided to individuals above, describe what privacy risks were identified and how you mitigated them.

The privacy risk associated with eGuardian is the lack of notice that information about individuals is being collected, used and maintained. The FBI has published a Privacy Act System of Records Notice (SORN) for FBI's investigative records, which provides general notice regarding entities with which and situations when the FBI may share investigative records. The FBI's routine uses for its systems and its Blanket Routine Uses provide further notice of the ways in which information collected by the FBI is shared. These notices, therefore, mitigate the privacy risk. No individual notice is provided, however, because the information in this system is collected by law enforcement and personal notice is not feasible.

Section 7.0
Individual Access and Redress

7.1 What are the procedures which allow individuals the opportunity to seek access to or redress of their own information?

Applicable regulations found in 28 CFR Part 16, Subparts A and D, which have been issued pursuant to the Freedom of Information and Privacy Acts, govern requests for access to information in FBI files. To the extent that other federal agencies, which contribute information to eGuardian, have processes in place to govern access or redress, those processes will apply to the information contributed by these agencies. As entries into eGuardian will most often be made by state and local law enforcement officers, the information may be retained in state and local agency records as well. Access to and opportunity to seek redress for those records is controlled by state law and procedures.

7.2 How are individuals notified of the procedures for seeking access to or amendment of their information?

28 C.F.R. 16.41 and 16.46 provide information on individual access and amendment of FBI records. Amendment of FBI records is a matter of discretion as the records are exempt from the Privacy Act amendment provisions.

7.3 If no opportunity to seek amendment is provided, are any other redress alternatives available to the individual.

See previous response.

7.4. Privacy Impact Analysis: Discuss any opportunities or procedures by which an individual can contest information contained in this system or actions taken as a result of agency reliance on information in the system.

Redress is generally not available except to the extent described in Section 7.2, above, but eGuardian is not intended to be a data repository, but a dynamic system where corrections and updates will be made as necessary during the short process of ascertaining whether a particular report merits further investigation because of a potential nexus to terrorism. If no nexus to terrorism is found, the SAR will be deleted from the system.

As a general matter, although FBI records are exempt from Privacy Act access and amendment procedures, the FBI strives to maintain accurate information and will, in its discretion, consider amendment requests.

Section 8.0
Technical Access and Security

8.1 Which user group(s) will have access to the system?

eGuardian access will be provided to State, local, and tribal law enforcement officers and agencies that have a law enforcement mission need for suspicious activity reports. Other federal law enforcement entities, including Department of Justice components, DHS and DoD entities with law enforcement missions, including force protection, will be provided access.

8.2 Will contractors to the Department have access to the system? If so, please submit a copy of the contract describing their role with this PIA.

Contractors will have access to the system in order to perform system maintenance and administration. In addition, to the extent contractors are assigned to any of the agencies that will have access to eGuardian, these individuals will also, upon proper vetting and clearances, be able to access the system.

8.3 Does the system use "roles" to assign privileges to users of the system?

Yes. eGuardian will have the following user roles:

1. Police Officer/Investigator/Intelligence Analyst/Support Contractor. These roles are generally reserved for individuals who create eGuardian incidents and are responsible for investigating and/or conducting analysis of terrorist-related threats and suspicious activity reports entered into the system. This role may include, at the discretion of the agency, an agency eGuardian supervisor who will control all eGuardian report dissemination from their agency. All such work will be electronically submitted to a coordinator at a responsible entity for review and authorization to be submitted into Guardian.

2. Coordinator/Administrator: The individual(s) assigned to this role works within the responsible entity to evaluate the information in eGuardian and performs other administrative functions with respect to the system. Individuals with this role have the ability to refer incidents to Guardian.

3. TMU will have overall administrative oversight of eGuardian and the capacity to monitor user roles assigned to each participating agency. Responsible entities will also exercise administrative oversight of users at their locations. With each participating agency, however, the determination of roles will be made locally.

8.4 What procedures are in place to determine which users may access the system and are they documented?

eGuardian will have restricted access and will follow a process regulated by TMU and by LEO. Prospective users must first clear the vetting requirements imposed by the LEO network, which include demonstrating that a proposed user is a member of an authorized law enforcement agency that is assigned an ORI or an agency with an operational necessity to share/receive information. In the event an agency with an operational necessity does not have an ORI, one will be created for that agency by the eGuardian developers/programmers, if appropriate. LEO revalidates all users' agency affiliation twice a year. Additionally, access to the eGuardian SIG will be controlled by TMU, which must approve all users. The procedures for system access are documented in policy and procedure documents developed by TMU for the eGuardian system.

8.5 How are the actual assignments of roles and rules verified, according to established security and auditing procedures?

Individual member agencies will be able to structure user roles and customize the work flow to fit their own needs. The responsible entities, however, will exercise administrative oversight of the system, which will include auditing for appropriate system access and use.

8.6 What auditing measures and technical safeguards are in place to prevent misuse of data?

Each user will have an individual account that requires a login and password for LEO. These accounts will be auditable. Each responsible entity, moreover, will have the responsibility to audit their users and will be obligated to report suspected misuse and security compromise. Rules of Behavior and training will cover the appropriate use of data and the penalties for misusing the information.

8.7 Describe what privacy training is provided to users either generally or specifically relevant to the functionality of the program or system?

As indicated previously, web-based training will be available to the user to assist with system access and procedure. In addition, eGuardian administrators from responsible entities will be provided classroom training that will emphasize their roles and responsibilities. A privacy statement will also be contained in the user agreement electronically signed by each participating agency.

8.8 Is the data secured in accordance with FISMA requirements? If yes, when was Certification and Accreditation last completed?

The Certification and Accreditation of the system is expected to be completed in early July and an Authority to Operate will be issued at that time.

8.9 Privacy Impact Analysis: Given access and security controls, what privacy risks were identified and how were they mitigated?

Privacy risks from this type of system stem from improper access and inadequate security. These risks have been mitigated in several ways. eGuardian access is based on role and function. In order to access the system, users must be sworn law enforcement officers or support personnel assigned to perform law enforcement analysis and/or criminal intelligence, as evidenced by an ORI. All users are vetted through LEO before they are permitted entry into the eGuardian Special Interest Group. Web-based training will be available to the user to assist with system access and procedures and the use of the information contained therein, with emphasis on privacy controls. Once an individual is vetted and authenticated through LEO, and then granted access to the eGuardian SIG, the individual's web-based session is controlled with computer software and hardware components secured behind accredited FBI security infrastructure. Placing eGuardian behind the FBI firewall and under the oversight of TMU will improve the security posture of the system.

Section 9.0
Technology

9.1 Were competing technologies evaluated to assess and compare their ability to effectively achieve system goals?

Yes. Several systems were reviewed and evaluated including an in-house solution. Final system design was based on operational imperatives and privacy and security attributes.

9.2 Describe how data integrity, privacy, and security were analyzed as part of the decisions made for your system.

Data integrity, privacy and security were important considerations in the development of this system. The task was to develop a robust information sharing system that would serve the needs of users for timely, relevant and accurate information in a secure environment while protecting privacy and ensuring data integrity and security. The system is designed to help investigators become aware of and make connections between reports of suspicious activities and terrorism threats in order to improve the security posture of the United States. Operationally the goal is to either close or refer for enhanced investigation all leads within a short period of time.

eGuardian is built upon and incorporates the lessons learned from the Guardian system and is designed to seamlessly interface with it. To enhance privacy protections for information that is added by SLT law enforcement personnel, a decision was made to use Fusion Centers as initial vetting points, as these groups can bring to bear enhanced information availability to ensure that suspicious activity reports and reports of incidents that have a potential nexus to terrorism meet a required threshold for system inclusion. TMU and a DOD fusion-like center will perform the same type of "fusion" for reports from federal entities. System functionality is designed to permit contributors to modify their entries as new information is received, and the need to check the system for updates will be incorporated as part of the required training for all users.

The eGuardian system was placed on an FBI server to enhance security and membership in the Special Interest Group of eGuardian users will be vetted through LEO, which performs this function for a variety of other law enforcement entities. User access will also be audited by TMU personnel.

9.3 What design choices were made to enhance privacy?

The eGuardian system is set up so that participating agencies can restrict the information they contribute in order to deny access to certain groups or individuals. This choice takes into account various state laws which have differing privacy requirements for sharing information and also allows contributors more control over their own information. A decision was also made to control access to reports in eGuardian to sworn law enforcement and analytical support personnel in order to ensure that those with training in handling sensitive law enforcement and terrorism-related information are the only ones who can access the system. The decision was made to use LEO as the hosting organization because it is an FBI-owned, web-based, sensitive but unclassified network that provides controlled access to facilitate information sharing. Placement of eGuardian on the Internet allows for ease of use but potentially exposes personally identifiable information to outside attack. LEO provides a restricted and more secure access to this information, which will enhance both privacy and security.

The work flow was created with privacy in mind so that contributors can easily update their information or mark it with a commentary to let other viewers know of particular issues pertaining to data integrity or privacy. Any re-dissemination of information will be subject to permission controls of the responsible or originating entity.

Conclusion

The eGuardian threat tracking system supports the FBI mission to prevent terrorist attacks on the United States. It is designed to mitigate and vet all threats and suspicious activities with a potential nexus to terrorism and assure they are properly addressed and available for trend analysis. Establishing an electronic system that will allow SLT and federal law enforcement partners to enter terrorist threat information and suspicious activity reports with a possible nexus to terrorism and share it with each other will facilitate the type of information sharing envisioned in the National Strategy for Information Sharing.

eGuardian has been designed in consultation with legal, privacy and security personnel in the FBI and elsewhere in order to ensure that privacy protections and security controls are integrated into system development and functionality. This privacy impact assessment is part of the process of ensuring that the system accounts for privacy concerns while creating an electronic environment that will facilitate operational imperatives.

Responsible Officials:

[redacted] 11/25/2008
Date

FBI Program Manager
Threat Monitoring Unit (TMU)
Federal Bureau of Investigation
[redacted]

[redacted] 11/25/2008
Date

FBI System Developer
Foreign Terrorist Tracking Task Force (FTTTF)
Federal Bureau of Investigation
[redacted]

b6
b7C

[redacted] 11/25/2008
Date

Chief Privacy and Civil Liberties Officer
Federal Bureau of Investigation

[redacted] 1/9/2009
Date

Chief Information Officer
Department of Justice

[redacted] 11/25/2008
Date

Acting Chief Privacy and Civil Liberties Officer
Department of Justice

Attachment 1

eGuardian User Agreement

Contact your local Joint Terrorism Task Force (JTTF) immediately by phone for any urgent matters with a potential nexus to terrorism.

eGuardian is a sensitive but unclassified system for official use only. Information classified CONFIDENTIAL and above cannot be placed into eGuardian under any circumstances. This includes all information that is SECRET, TOP SECRET OR COMPARTMENTED. Neither FISA-derived information nor Grand Jury 6(e) material nor any other information that is legally restricted may be placed into eGuardian.

The suspicious activities contained in eGuardian may be raw and unvetted data. "Suspicious activity is defined by the Program Manager of the Information Sharing Environment (PM/ISE) as observed behavior that may be indicative of intelligence gathering or pre-operational planning related to terrorism, criminal or other illicit intention. Suspicious activities may include, but are not limited to, surveillance, cyber attacks, probing of security and photography of key infrastructures and facilities. Do not conduct any unilateral investigation with any reported incident without the coordination of the originating agency/author. Do not arrest any individual based solely on the information in eGuardian unless there is evidence of a violation of State, Local or Federal statutes.

By signing the user agreement, the parties will agree to the Fusion Center and TMU policy that sets forth the mission, goals, functions, management, principles, membership, staffing, information sharing policies and protocols and privacy and security attributes of the eGuardian system.

Membership in the SIG is by application only and will be drawn only from agencies that have an originating agency identifier (ORI) and thus are recognized law enforcement entities.

No entry into eGuardian may be made based solely on the ethnicity, race or religion of an individual or solely on the exercise of rights guaranteed by the First Amendment or the lawful exercise of any other rights secured by the Constitution or laws of the United States.

If you determine that information you have previously submitted is erroneous, you are responsible for updating or correcting the information in eGuardian. If you discover information that has been contributed that you know is erroneous, you should notify the submitter so that the information can be corrected.

Proceeding to the eGuardian Threat Tracking System indicates you have been informed of, agree to, and will abide by these restrictions. Incidents not meeting the criteria of suspicious activities or with a potential nexus to terrorism and that, further, do not comply with the above-stated rules, will be immediately deleted from eGuardian. Furthermore, by clicking on the User Agreement check box, you agree to the policies that govern the eGuardian system. For further information about the eGuardian policy, please return to the policy link on the LEO eGuardian member area page.

Information obtained through eGuardian shall not be re-disseminated without the approval of a responsible entity or the originating entity.

The TMU will conduct periodic audits of the system to ensure that the rules are followed. Failure to comply with this agreement will result in the termination of your eGuardian membership.

Exhibit F

ROLL CALL RELEASE

In Collaboration with the ITACG

26 July 2010

(U//FOUO) Indicators of Suspicious Behaviors at Hotels

(U//FOUO) Known or possible terrorists have displayed suspicious behaviors while staying at hotels overseas—including avoiding questions typically asked of hotel registrants; showing unusual interest in hotel security; attempting access to restricted areas; and evading hotel staff. These behaviors also could be observed in U.S. hotels, and security and law enforcement personnel should be aware of the potential indicators of terrorist activity.

(U//FOUO) **Possible indicators of terrorist behaviors at hotels:** The observation of multiple indicators may represent—based on the specific facts or circumstances—possible terrorist behaviors at hotels:

- (U//FOUO) Not providing professional or personal details on hotel registrations—such as place of employment, contact information, or place of residence.
- (U//FOUO) Using payphones for outgoing calls or making front desk requests in person to avoid using the room telephone.
- (U//FOUO) Interest in using Internet cafes, despite hotel Internet availability.
- (U//FOUO) Non-VIPs who request that their presence at a hotel not be divulged.
- (U//FOUO) Extending departure dates one day at a time for prolonged periods.
- (U//FOUO) Refusal of housekeeping services for extended periods.
- (U//FOUO) Extended stays with little baggage or unpacked luggage.
- (U//FOUO) Access or attempted access to areas of the hotel normally restricted to staff.
- (U//FOUO) Use of cash for large transactions or a credit card in someone else's name.
- (U//FOUO) Requests for specific rooms, floors, or other locations in the hotel.
- (U//FOUO) Use of a third party to register.
- (U//FOUO) Multiple visitors or deliveries to one individual or room.
- (U//FOUO) Unusual interest in hotel access, including main and alternate entrances, emergency exits, and surrounding routes.
- (U//FOUO) Use of entrances and exits that avoid the lobby or other areas with cameras and hotel personnel.
- (U//FOUO) Attempting to access restricted parking areas with a vehicle or leaving unattended vehicles near the hotel building.
- (U//FOUO) Unusual interest in hotel staff operating procedures, shift changes, closed-circuit TV systems, fire alarms, and security systems.
- (U//FOUO) Leaving the property for several days and then returning.
- (U//FOUO) Abandoning a room and leaving behind clothing, toiletries, or other items.
- (U//FOUO) Noncompliance with other hotel policies.

FOR POLICE, FIRE, EMS, and SECURITY PERSONNEL

IA-0395-10

(U) Prepared by the DHS/I&A Homeland Counterterrorism Division, the DHS/I&A Cyber, Infrastructure, and Science Division, the FBI/Directorate of Intelligence, and the Interagency Threat Assessment and Coordination Group. This product is intended to assist federal, state, local, and private sector first responders so they may effectively deter, prevent, preempt, or respond to terrorist attacks against the United States. This product was coordinated with the DHS/Office of Infrastructure Protection.

*(U) **Warning:** This document is UNCLASSIFIED//FOR OFFICIAL USE ONLY (U//FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information and is not to be released to the public, the media, or other personnel who do not have a valid need to know without prior approval of an authorized DHS official. State and local homeland security officials may share this document with critical infrastructure and key resource personnel and private sector security officials without further approval from DHS.*

(U) The FBI regional phone numbers can be found online at http://www.fbi.gov/contact/fo/fo.htm and the DHS National Operations Center (NOC) can be reached by telephone at (202) 282-9685 or by e-mail at NOC.Fusion@dhs.gov. For information affecting the private sector and critical infrastructure, contact the National Infrastructure Coordinating Center (NICC), a sub-element of the NOC. The NICC can be reached by telephone at (202) 282-9201 or by e-mail at NICC@dhs.gov.

Exhibit G

The FBI's Terrorism Quick Reference Card

First responding officers should be aware of suspicious factors that may indicate a possible terrorist threat. These factors should be considered collectively in assessing a possible threat. This quick reference guide is intended to provide practical information for line officers but may not encompass every threat or circumstance. State and local law enforcement may contact their local FBI field office or resident agency for additional assistance.

1) Possible Suicide Bomber Indicators -A.L.E.R.T.

A. **A**lone and nervous.
B. **L**oose and/or bulky clothing (may not fit weather conditions).
C. **E**xposed wires (possibly through sleeve).
D. **R**igid mid-section (explosive device or may be carrying a rifle).
E. **T**ightened hands (may hold detonation device).

2) Passport History

A. Recent travel overseas to countries that sponsor terrorism.
B. Multiple passports with different countries/names (caution: suspect may have dual citizenship).
C. Altered passport numbers or photo substitutions; pages have been removed.

3) Other Identification -Suspicious Characteristics

A. No current or fixed address; fraudulent/altered: Social Security cards, visas, licenses, etc.; multiple ID's with names spelled differently.
B. International drivers ID:

1. There are no international or UN drivers' licenses -they are called permits.

2. Official international drivers' permits are valid for one year from entry into the U.S., they are paper-gray in color, not laminated, and are only valid for foreign nationals to operate in the U.S.

4) Employment/School/Training

A. No obvious signs of employment.
B. Possess student visa but not English proficient.
C. An indication of military type training in weapons or self-defense.

5) Unusual Items In Vehicles/Residences

A. Training manuals; flight, scuba, explosive, military, or extremist literature.
B. Blueprints (subject may have no affiliation to architecture).
C. Photographs/diagrams of specific high profile targets or infrastructures; to include entrances/exits of buildings, bridges, power/water plants, routes, security cameras, subway/sewer, and underground systems.
D. Photos/pictures of known terrorists.
E. Numerous prepaid calling cards and/or cell phones.
F. Global Positioning Satellite (GPS) unit
G. Multiple hotel receipts
H. Financial records indicating overseas wire transfers
I. Rental vehicles (cash transactions on receipts; living locally but renting)

The FBI's Terrorism Quick Reference Card -- Continued

6) Potential Props

A. Baby stroller or shopping cart.
B. Suspicious bag/backpack, golf bag.
C. Bulky vest or belt.

7) Hotel/Motel Visits

A. Unusual requests, such as:
  1. Refusal of maid service.
  2. Asking for a specific view of bridges, airports, military/government installation (for observational purposes).
  3. Electronic surveillance equipment in room
B. Suspicious or unusual items left behind.
C. Use of lobby or other pay phone instead of room phone.

8) Recruitment Techniques

CAUTION: The following factors, which may constitute activity protected by the United States Constitution, should only be considered in the context of other suspicious activity and not be the sole basis of law enforcement action.

A. Public demonstrations and rallies.
B. Information about new groups forming.
C. Posters, fliers, and underground publications.

9) Thefts, Purchases, Or Discovery Of:

A. Weapons/explosive materials.
B. Camera/surveillance equipment.
C. Vehicles (to include rentals - fraudulent name; or failure to return vehicle).
D. Radios: Short wave, two-way and scanners.
E. Identity documents (State IDs, passports etc.)
F. Unauthorized uniforms

II. Indicators and Detection of Terrorist Explosive/Weapons/CBN Attack[1]

1. Possible Explosive Attack Indicators

- Theft of commercial-grade explosives, chemical substances, blasting caps.
- Large amounts of high-nitrate fertilizer sales to nonagricultural purchasers, or abnormally large amounts (compared with previous sales) to bona fide agricultural purchasers.
- Large theft or sales of chemicals which, when combined, create ingredients for explosives (fuel oil, nitrates).
- Theft or abnormal sales of containers (for example, propane bottles) or possible vehicles (trucks or cargo vans) in combination with other indicators.
- Reports of explosions where not authorized.
- Seizures of improvised explosive devices or materials.

2. Possible Weapons Attack Indicators

- Theft or unusual sales of large numbers of semi-automatic weapons, especially those which are known to be readily converted to fully-automatic.
- Theft or unusual sales of military-grade weapons ammunition.
- Reports of automatic weapons firing.
- Seizures of modified weapons or equipment used to modify weapons (especially silencers).
- Theft, sales, or seizure of night vision or thermal imaging equipment when combined with other indicators.
- Theft, loss, seizure, or recovery of large amounts of cash by groups advocating violence against the government, military, or similar targets.

3. Possible Chemical/Biological/Nuclear Indicators:

- Sales or theft of large quantities of baby formula, or an unexplained shortage in an area. (Baby formula is used to grow certain specific cultures.)
- Break-in or tampering with equipment at water treatment facilities or food processing facilities or warehouses.
- Theft or solicitation for sales of live agents, toxins, or diseases from medical supply companies or testing and experimentation facilities.
- Multiple cases of unexplained human or animal deaths.
- Sales to non-agricultural users or thefts of agricultural sprayers, or crop-dusting aircraft, foggers, river craft or other dispensing systems.
- Inappropriate inquiries regarding local chemical/biological/nuclear sales, storage, or transportation points and facilities.
- Inappropriate inquiries regarding heating and ventilation systems for buildings or facilities by persons not associated with service agencies.

III. Surveillance, Targeting, and Attack Indicators and Countermeasures

A. Surveillance[2]

According to the Department of Homeland Security, nearly every major terrorist attack has been preceded by a thorough surveillance of the targeted facility. **Surveillance operations have certain characteristics that are particular to pre-operational activity.** The degree of expertise used in the execution of the operation will increase or decrease the likelihood of detection. Some of these characteristics are:

- Suspicious persons or vehicles being observed in the same location on multiple occasions, including those posing as panhandlers, vendors, or others not previously seen in the area.
- Suspicious persons sitting in a parked car for an extended period of time for no apparent reason.
- Personnel observed near a potential target using or carrying video, still camera, or other observation equipment, especially when coupled with high magnification lenses.
- Suspicious persons showing an interest in or photographing security systems and positions.
- Personnel observed with facility maps and/or photographs, or diagrams with specific buildings or facilities highlighted; or with notes regarding infrastructure, or listing of certain key personnel.
- Suspicious persons drawing pictures or taking notes in a non-tourist or other area not normally known to have such activity.
- Personnel possessing or observed using night vision or thermal devices near the potential target area
- Personnel observed parked near, standing near, or loitering near the same vicinity over several days, with no apparent reasonable explanation.
- A noted pattern or series of false alarms requiring law enforcement or emergency services response; individuals noticeably observing security procedures and responses or questioning security or facility personnel.
- Persons not fitting into the surrounding environment, such as wearing improper attire for the location.
- Theft of official identification (ID) cards (including family members, retirees), or government official license plates.
- Non-government persons in possession of government official ID cards.
- Recent damage to potential target perimeter security (breaches in the fenceline).
- Computer hackers attempting to access sites with personal information, maps, or other data useful to compiling a target information packet.
- Persons exhibiting unusual behavior such as staring or quickly looking away from individuals or vehicles as they enter or leave designated facilities or parking areas.
- A blank facial expression in an individual may be indicative of someone concentrating on something not related to what they appear to be doing.

III. Surveillance, Targeting, and Attack Indicators and Countermeasures -- Continued

B. Targeting[3]

If the intended target of an operation is an individual, the information collected on that person may include several of the following:

- The identity, age, residence, and social status of the intended target.
- A description of the vehicle that the target drives.
- The work environment of the intended target, to include time of departure and return from work as well as the route taken to his/her place of employment.
- The manner in which the target spends his/her free time and the places where he/she spends vacations and holidays.
- The identity and address of the target's friends.
- The identity of the target's spouse, where he/she works and whether the target visits him/her there.
- The identity of the target's children and whether the target visits at the school.
- Whether the target has a significant other (boyfriend or girlfriend), that person's address, and when the target visits there.
- The identity of the physician who treats the target.
- The location of the stores where the target does his/her shopping.
- The location of entrances and exits to the target's residence, and the surrounding streets.
- Means of surreptitiously entering the target's residence.
- Whether the target is armed; if protected by guards, the number of guards and their armament, if any.

If the intended target is a facility or important building, surveillance teams may attempt to obtain the following information pertaining to the exterior of the facility:

- The width of the streets and the direction in which they run leading to the facility.
- Available transportation to the facility.
- The area, physical layout, and setting of the facility.
- Traffic signals and pedestrian areas near the facility.
- The location of security personnel centers (police stations, etc.) and nearby government agencies.
- The economic characteristics of the area where the place is located.
- Traffic congestion times near the facility.
- Amount and location of lighting near the facility.

Surveillance teams may also attempt to obtain the following information pertaining to the interior of the facility:

- Number of people typically inside the facility.
- Number and location of guard posts within the facility.
- Number and names of the leaders within the facility.
- Number of floors and rooms within the facility.
- Telephone lines and the location of the switchboard.
- Times of entrance and exit of specific individuals.
- Inside parking available at the facility.
- Location of electrical power switches.

III. Surveillance, Targeting, and Attack Indicators and Countermeasures -- Continued

Training literature also identifies **the use of photography and detailed drawings by those conducting surveillance operations**. Photographs are taken to depict panoramic and overlapping views of potential target areas. Surveillance team members typically also draw a diagram of the target of the surveillance operation. The diagram is typically realistic so that someone who never saw the target could visualize it. In order for the diagram to accurately depict the target it should contain the following:

- Shapes and characteristics of buildings and surrounding features.
- Traffic directions and width of streets.
- Location of traffic signals and pedestrian areas.
- Location of police stations, security personnel centers and government agencies.
- Location of public parks.
- Amount and location of lighting.

C. Attack[4]

Pre-Attack Indicative Behaviors:

- Making threats directly to the target or indirectly to third parties.
- "Leakage" by attacker (behavioral signs of intent to attack), including:
  - vague threats (to manage own emotions of anger, anxiety, or fear);
  - bragging to third parties of intent to attack;
  - exaggerated, larger-than-life articulated fantasies of success or outcome of bombing (e.g., number of victims, joining other martyrs that have preceded him);
  - evasive when questioned concerning past history and future plans, or such information is not realistic or verifiable.
- Casing of properties/buildings.

Pre-Attack Countermeasures:

- Proactively pursue through investigation and questioning any individual reported to be a threat to bomb or carry out a terrorist act and thereby arouse suspicions in others.
- Interview collaterals (family, friends, employers, neighbors and co-religionists) who observe changes in the individual's behavior (withdrawal from previous social contacts; radicalization of beliefs; travel to countries know to be supportive of terrorist activities; associations with other suspected terrorists; new and unidentified sources of income; increase in religiousness).
- Gather intelligence in communities containing or supporting such activity.
- Develop and acquire assets among trusted community resources (local media, religious leaders, community activists, and professionals).

Attack Preparation: Indicative Behaviors

- No direct threats to the target, but continues to communicate threat to trusted third parties.
- "Leakage" may continue to third parties, but may become more constricted on advice of higher-ups.
- "Boundary probing" with physical approaches to measure restrictions to access, if any (private security, physical boundaries, local law enforcement presence).
- Surveillance of target (victims and location); familiarization with area, decision making concerning dress and appearance, and select time and day to maximize casualties; counter-surveillance of security personnel or barriers already in place.
- Acquisition of materials for the bomb, including the explosive proper, the detonation device, and the container. The latter may be selected on the basis of commonly seen packages or items in the target area (backpacks, grocery bags, retail bags) derived from surveillance.
- May prepare a suicide note or video for dissemination after the bombing.
- May give possessions away and get other worldly affairs in order.

III. Surveillance, Targeting, and Attack Indicators and Countermeasures -- Continued

- Emotions are likely to be more volatile (quickly changing; may be irritable, sad, easily upset).
- May indulge in "worldly sins" that directly violate religious beliefs (visiting bars, strip clubs, gambling) in order to blend in with victims and avoid apprehension.
- Will pay for items in cash.
- Daily behaviors become consistent with no future (e.g., forgetting to take change, purchasing one-way tickets).
- Handler's involvement increases to help suicide bomber stay focused and manage anxiety; chief communication will be through e-mail, cell phone, or direct contact.
- May show arrogance and hatred toward Americans through bragging, expressed dislike of attitudes and decisions of US government, superiority of religious beliefs, and difficulty tolerating proximity to those hates (e.g., waiting in a grocery store line becomes intolerable).
- Will engage in "private rituals" within hours of the bombing that have religious and symbolic meaning, such as bathing, fasting, shaving of body hair, perfuming, and increased praying. These acts reinforce the meaning of his suicide bombing, steal him to the task, and keep him focused on the larger cause.

Attack Preparation Countermeasures

- Actively interview suspects and close contacts reported to be engaging in preparation to attack.
- Detain and/or arrest, if probable cause to do so exists, to prevent further preparation and attack.
- Conduct "warehouse surveys" of retail outlets for bomb making materials to identify the suspect's acquisition behavior and gather evidence (e.g., computer stores, Radio Shack or other electronic instrument stores, and chemical ingredient or fertilizer outlets).
- Conduct counter-surveillance of the identified target.
- Harden the identified target to reduce or impede access by a suicide bomber or other suicide terrorists.
- Monitor e-mail or cell phone usage of the suspect bomber.
- Continue surveillance of the suspect's behavior.

Attack Initiation: Indicative Behaviors:

- Clothing is out of sync with the weather, suspect's social position (he appears well-groomed but is wearing sloppy clothing), or location (wearing a coat inside a building).
- Clothing is loose.
- Suspect may be carrying heavy luggage, bag, or wearing a backpack.
- Suspect sometimes keeps his hands in his pockets.
- Suspect repeatedly pats his upper body with his hands, as if double-checking whether he forgot something.
- Pale face from recent shaving of beard.
- No obvious emotion seen on the face.
- Eyes appear to be focused and vigilant. Does not respond to authoritative voice commands or direct salutation from a distance.
- May appear to be "in a trance."
- Suspect walks deliberately but is not running.
- Just prior to detonation, suspect will hold his hands above his head and shout a phrase; or suspect will place his hands and head close to the bomb to obliterate post-mortem identification.

III. Surveillance, Targeting, and Attack Indicators and Countermeasures -- Continued

Attack Initiation Countermeasures:

- Call or shout a voice command from a distance to break the suspect's concentration.
- Make physical contact with the suspect to distract his attention and physically impede his forward movement.
- Insure physical control before questioning, especially of hands and arms.
- Insure safety of civilian targets in immediate area.

Post Offense Behavior by Attacker's Handlers or Associates: Indicative Behaviors:

- Synchronized serial attacks implemented in stages, in close physical or temporal proximity to increase casualties of first responders, including law enforcement and medical personnel.
- If there is a second attack, it is likely to occur within 20 minutes and be carried out along evacuation route of casualties or near first targeted area.
- Surveillance of attack site to study first responders' behavior and plan for future attacks.

Post Offense Countermeasures:

- Make counter-surveillance team a part of the first response.
- Include bomb disposal experts in first response to search for additional explosives.

[1] Source: Chief Warrant Officer 3 Del Stewart, U.S. Army Intelligence Center

[2] Source: Chief Warrant Officer 3 Del Stewart, U.S. Army Intelligence Center; FBI Intelligence Bulletin 53, February 26, 2003, "Possible Indicators of al-Qaeda Surveillance."

[3] This section extracted from "Use of Surveillance by Terrorist Groups," by the CONUS Analysis Section, Pol Mil/Force Protection Branch, Joint Forces Intelligence Command

[4] This section extracted from "Suicide/Homicide Attacker Behaviors and Suggested Countermeasures," by FBI Behavioral Analysis Program & Central Intelligence Agency analysts, and issued by the Interagency Intelligence Committee on Terrorism.

Exhibit H

BJA Bureau of Justice Assistance

Communities Against Terrorism

Potential Indicators of Terrorist Activities Related to the General Public

What Should I Consider Suspicious?

People involved in terrorist activity often exhibit indicators that if observed could identify a potential impending crime or terrorist attack. The following is a list of some of the characteristics of such persons that you should be aware of .

- Unusual requests for information –
  - questions regarding sensitive information such as security procedures or systems
  - questions regarding facility operations
- Unusual interest in high risk or symbolic targets
  - surveillance
  - note taking
  - drawing of diagrams
  - annotating maps
  - inappropriate photographs or videos
  - people over dressed for the weather
- Unusual activity –
  - people acting suspiciously
  - people departing quickly when seen or approached
  - people in places where they do not belong
  - vehicles that appear to be overloaded

What Should I Do?

It is important to give a thorough report when notifying law enforcement. Keep in mind the responding officer may only have the information you gave at the time of your call. Providing a detailed description of persons or vehicles is imperative for a successful follow up by law enforcement personnel.

If something seems wrong, notify law enforcement authorities.

Do not jeopardize your safety or the safety of others.

Columbus, Ohio Division of Police
Homeland Security Section
Terrorism Early Warning Unit
614-645-5410
1-866-759-8005

Help Protect Your Community

Be Part of the Solution

BJA Bureau of Justice Assistance

Terrorism may be national or international in scope, but terrorist incidents occur locally and are preceded by a number of pre-incident activities. Individuals in the community are key to identifying these pre-incident activities. By learning what to look for, **you** can aid law enforcement officials in protecting the homeland.

By being aware of what to look for and knowing how to report suspicious behavior, **you** can make a positive contribution in the fight against terrorism. The **partnership between the community and law enforcement** is essential to the success of anti-terrorism efforts.

It is important to remember that just because someone's speech, actions, beliefs, appearance, or way of life is different, it does not mean that he or she is suspicious. Instead, focus on behavior and activities that are unusual or out of place for the situation and that appear to be suspicious.

The activities outlined on this handout are by no means all-inclusive but have been compiled from a review of terrorist events over several years. Some of the activities, taken individually, could be innocent and must be examined by law enforcement professionals in a larger context to determine whether there is a basis to investigate.

This project was supported by Grant Number 2007-MU-BX-K002, awarded by the Bureau of Justice Assistance, Office of Justice Programs, U.S. Department of Justice. The opinions, findings, and conclusions or recommendations expressed in this document are those of the authors and do not necessarily represent the official position or policies of the U.S. Department of Justice.

Potential Indicators of Terrorist Activities Related to the General Public

Columbus, Ohio Division of Police
Homeland Security Section
Terrorism Early Warning Unit
614-645-5410
1-866-759-8005

Exhibit I

BJA Bureau of Justice Assistance

FBI Federal Bureau of Investigation

Communities Against Terrorism

Potential Indicators of Terrorist Activities Related to Electronic Stores

What Should I Consider Suspicious?

People Who:

- Significantly alters appearance from visit to visit (shaving beard, changing hair color, style of dress, etc)
- Missing hand/fingers, chemical burns, strange odors or bright colored stains on clothing
- Fills a "shopping list" of components lacking knowledge about specifications and uses
- Purchases quantities of prepaid or disposable cell phones
- Insists prepaid phones not be activated or programmed upon purchase
- Pays cash for large purchases; uses credit card(s) in different name(s), uses suspicious identification
- Travels illogical distance to purchase items or asks where similar stores are located

Purchasers showing unusual interest through questions related to:

- Radio frequencies (used/not used) by law enforcement
- Voice or data encryption, VOIP, satellite phones, voice privacy
- Use of anonymizers, portals, or other means to shield IP address
- Swapping SIM cards in cell phones or how phone location can be tracked
- Rewiring cell phone's ringer or backlight
- Products/components related to military-style equipment
- Unusual comments regarding radical theology, vague/cryptic warnings, or anti-U.S. sentiments that appear to be out-of-place and provocative

Purchases including unusual combinations of:

- Electronic timer or timing devices
- 2-way radios
- GPS
- Digital Voice Changers
- Infra-Red Devices
- Police scanners
- Phone or "bug" detection devices
- Batteries
- Switches
- Wire and soldering tools
- Night Vision
- Flashlight Bulbs

It is important to remember that just because someone's speech, actions, beliefs, appearance, or way of life is different; it does not mean that he or she is suspicious.

What Should I Do?

Be part of the solution.

- ✓ Require valid ID from all new customers.
- ✓ Keep records of purchases.
- ✓ Talk to customers, ask questions, and listen to and observe their responses.
- ✓ Watch for people and actions that are out of place.
- ✓ Make note of suspicious statements, people, and/or vehicles.
- ✓ **If something seems wrong, notify law enforcement authorities.**

Do not jeopardize your safety or the safety of others.

Preventing terrorism is a community effort. By learning what to look for, **you** can make a positive contribution in the fight against terrorism. The **partnership between the community and law enforcement** is essential to the success of anti-terrorism efforts.

Some of the activities, taken individually, could be innocent and must be examined by law enforcement professionals in a larger context to determine whether there is a basis to investigate. The activities outlined on

Joint Regional Intelligence Center (JRIC)
www.jric.org

(888) 705-JRIC (5742) mention "Tripwire"

This project was supported by Grant Number 2007-MU-BX-K002, awarded by the Bureau of Justice Assistance, Office of Justice Programs, U.S. Department of Justice. Each indictor listed above, is by itself, lawful conduct or behavior and may also constitute the exercise of rights guaranteed by the U.S. Constitution. In addition, there may be a wholly innocent explanation for conduct or behavior that appears suspicious in nature. For this reason, no single indicator should be the sole basis for law enforcement action. The totality of behavioral indicators and other relevant circumstances should be evaluated when considering any law enforcement response or action.

Exhibit J

BJA Bureau of Justice Assistance

FBI Federal Bureau of Investigation

Communities Against Terrorism

Potential Indicators of Terrorist Activities Related to Mass Transportation

What Should I Consider Suspicious?

Related to Individual Appearance, General Behavior, and Communications:

- Significantly alters appearance from visit to visit (shaving beard, changing hair color, style of dress, etc)
- Burns on body, missing finger(s) or hand, bloody clothing, bleached body hair or bright colored stains on clothing; switch or wires concealed in hand, clothing or backpack
- Passing anonymous threats (telephone/e-mail) to facilities in conjunction with suspected surveillance incidents
- Acting nervous or suspicious, possibly mumbling to themselves, heavy sweating
- Monitoring personnel or vehicles entering/leaving facilities or parking areas
- Behaving as if using a hidden camera (panning a briefcase/bag over a particular area or constantly adjusting angle or height of an item)
- Discreetly using cameras, video recorders, binoculars, or note taking and sketching
- Unusual comments made regarding anti-U.S., radical theology, vague or cryptic warnings
- Questioning security/facility personnel through personal contact, telephone, mail, or e-mail

Related to Passenger Activities or Interests in Security:

- Multiple people arriving together, splitting up; may continue to communicate via cell phone
- Unusual or prolonged interest in the following:
  - Security measures or personnel
  - Security cameras
  - Entry points and access controls
  - Perimeter barriers (fences/walls)
  - Unattended train or bus
- Parking vehicles in restricted zones or purposely placing objects in sensitive or vulnerable areas to observe security responses
- Attempting to acquire official vehicles, uniforms, badges, access cards, or identification credentials for key facilities (report such losses and deactivate access cards immediately)
- Observing security reaction drills or procedures (may leave an unattended package to probe)

It is important to remember that just because someone's speech, actions, beliefs, appearance, or way of life is different; it does not mean that he or she is suspicious.

Joint Regional Intelligence Center (JRIC)
www.jric.org
(888) 705-JRIC (5742) mention "Tripwire"

What Should I Do?

Be part of the solution.

- ✓ Require valid ID from all customers.
- ✓ Keep records of purchases.
- ✓ Talk to customers, ask questions, and listen to and observe their responses.
- ✓ Watch for people and actions that are out of place.
- ✓ Make note of suspicious statements, people, and/or vehicles.
- ✓ **If something seems wrong, notify law enforcement authorities.**

Do not jeopardize your safety or the safety of others.

Preventing terrorism is a community effort. By learning what to look for, **you** can make a positive contribution in the fight against terrorism. The **partnership between the community and law enforcement** is essential to the success of anti-terrorism efforts.

Some of the activities, taken individually, could be innocent and must be examined by law enforcement professionals in a larger context to determine whether there is a basis to investigate. The activities outlined on this handout are by no means all-inclusive but have been compiled from a review of terrorist events over several years.

This project was supported by Grant Number 2007-MU-BX-K002, awarded by the Bureau of Justice Assistance, Office of Justice Programs, U.S. Department of Justice. Each indictor listed above, is by itself, lawful conduct or behavior and may also constitute the exercise of rights guaranteed by the U.S. Constitution. In addition, there may be a wholly innocent explanation for conduct or behavior that appears suspicious in nature. For this reason, no single indicator should be the sole basis for law enforcement action. The totality of behavioral indicators and other relevant circumstances should be evaluated when considering any law enforcement response or action.